

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 1999年 5月27日

出 願 番 号
Application Number: 平成11年特許願第147663号

パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願
番号

The country code and number
of your priority application,
to be used for filing abroad
under the Paris Convention, is

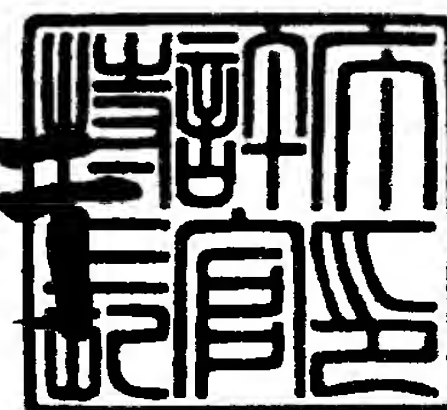
J P 1 9 9 9 - 1 4 7 6 6 3

出 願 人
Applicant(s): 株式会社日立製作所

2010年11月 4日

特許庁長官
Commissioner,
Japan Patent Office

岩井良行



【書類名】 特許願

【整理番号】 H99012941A

【提出日】 平成11年 5月27日

【あて先】 特許庁長官 殿

【国際特許分類】

H04L 12/56

H04L 12/46

【発明者】

【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目280番地 株式
会社日立製作所中央研究所内

【氏名】 坂本 健一

【発明者】

【住所又は居所】 神奈川県秦野市堀山下1番地 株式
会社日立製作所エンタープライズサーバ事業部内

【氏名】 星野 和義

【発明者】

【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目280番地 株式
会社日立製作所中央研究所内

【氏名】 若山 浩二

【発明者】

【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目280番地 株式
会社日立製作所中央研究所内

【氏名】 田辺 史朗

【発明者】

【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目280番地 株式
会社日立製作所中央研究所内

【氏名】 遠藤 昇

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社日立製作所

【代理人】

【識別番号】 100075096

【弁理士】

【氏名又は名称】 作田 康夫

【電話番号】 03-3212-1111

【手数料の表示】

【予納台帳番号】 013088

【納付金額】 21,000

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 VPN構成方式、インターワークルータ装置、パケット通信方法、データ通信装置及びパケット中継装置

【特許請求の範囲】

【請求項 1】

可変長パケットにより通信を行うユーザに対してパケット通信サービスを提供するための第一の通信網と、

同様に可変長パケットにより通信を行うユーザに対してパケット通信サービスを提供するための第一の通信網があり、

前記第一の通信網では、特定のユーザのパケットを他のユーザのパケットと混合させない閉域網を構成するために、前記通信網の内部では可変長パケットに対して網内を転送するために特別に付与する第一のカプセルヘッダを網の入り口で付与し、網の出口で削除する構成を持ち、

前記第二の通信網でも同様に、特定のユーザのパケットを他のユーザのパケットと混合させない閉域網を構成するために、前記通信網の内部では可変長パケットに対して網内を転送するために特別に付与する第二のカプセルヘッダを網の入り口で付与し、網の出口で削除する構成を持ち、

前記第一の通信網と前記第二の通信網の接続点では、第一の通信網から第二の通信網に転送される特定のユーザのパケットに対しては、第一のカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、第二の通信網への方路選択及び第二の通信網で使用する第二のカプセルヘッダを生成し、

第二の通信網から第一の通信網に転送される特定のユーザのパケットに対しては、第二のカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、第二の通信網への方路選択及び第一の通信網で使用する第二のカプセルヘッダを生成することにより、

第一の網及び第二の網にまたがる閉域網を構成することを特徴とする、可変長パケット通信によるVPN (Virtual Private Network) 構成方式。

【請求項 2】

可変長パケット通信方式にインターネットプロトコルを用いることを特徴とし

た請求項 1 に記載の V P N 構成方式。

【請求項 3】

第一の網または第二の網のカプセル化ヘッダとして、インターネットプロトコルによるカプセルヘッダを用いることを特徴とした請求項 2 記載の V P N 構成方式。

【請求項 4】

第一の網または第二の網のカプセル化ヘッダとして、インターネットプロトコルの下位レイヤにあたる、A T M 通信方式のヘッダを使用することを特徴とした請求項 2 記載の V P N 構成方式。

【請求項 5】

第一の網または第二の網のカプセル化ヘッダとして、インターネットプロトコルの下位レイヤにあたる、H D L C (P P P、フレームリレー) 通信方式のヘッダを使用することを特徴とした請求項 2 記載の V P N 構成方式。

【請求項 6】

第一の網または第二の網のカプセル化ヘッダとして、インターネットプロトコルの下位レイヤにあたる、M P L S (Multi-Protocol Layer Switching) 通信方式のヘッダを使用することを特徴とした請求項 2 記載の V P N 構成方式。

【請求項 7】

可変長パケットにより通信を行うユーザに対してパケット通信サービスを提供し、特定のユーザのパケットを他のユーザのパケットと混合させない閉域網を構成するために、前記通信網の内部では可変長パケットに対して網内を転送するために特別に付与する第一のカプセルヘッダを網の入り口で付与し、網の出口で削除する構成を持ち、閉域網を構成することのできる複数の通信網があり、それぞれの接続点では、第一の通信網から第二の通信網に転送される特定のユーザのパケットに対しては、第一のカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、第二の通信網への方路選択及び第二の通信網で使用する第二のカプセルヘッダを生成し、第二の通信網から第一の通信網に転送される特定のユーザのパケットに対しては、第二のカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、第二の通信網への方路選択及び第一の通信網で使用する第二

のカプセルヘッダを生成することにより 2 つの通信網にまたがる閉域網を構成することにより、複数網にまたがる閉域網を構成することを特徴とする V P N 構成方式。

【請求項 8】

可変長パケット通信方式にインターネットプロトコルを用いることを特徴とした請求項 7 に記載の V P N 構成方式。

【請求項 9】

それぞれの網で使用されるカプセル化ヘッダとして、インターネットプロトコルによるカプセルヘッダを用いることを特徴とした請求項 8 記載の V P N 構成方式。

【請求項 1 0】

それぞれの網で使用されるカプセル化ヘッダとして、インターネットプロトコルの下位レイヤにあたる、A T M 通信方式のヘッダを使用することを特徴とした請求項 8 記載の V P N 構成方式。

【請求項 1 1】

それぞれの網で使用されるカプセル化ヘッダとして、インターネットプロトコルの下位レイヤにあたる、H D L C (P P P、フレームリレー) 通信方式のヘッダを使用することを特徴とした請求項 8 記載の V P N 構成方式。

【請求項 1 2】

それぞれの網で使用されるカプセル化ヘッダとして、インターネットプロトコルの下位レイヤにあたる、M P L S (Multi-Protocol Layer Switching) 通信方式のヘッダを使用することを特徴とした請求項 8 記載の V P N 構成方式。

【請求項 1 3】

それぞれの網において使用されるカプセル化ヘッダ内にパケット転送の優先度クラスを持ち、2 つの網の接続点では、パケットが転送されてきた第一の網で使用されている前記カプセル化ヘッダ内の前記優先度クラスの情報にパケットが転送されていく第二の網で使用されている前記カプセル化ヘッダ内の優先度クラスの領域にマッピングを行うことを特徴とする請求項 1 に記載の V P N 構成方式。

【請求項 1 4】

それぞれの網において使用されるカプセル化ヘッダ内にパケット転送の優先度クラスを持ち、2つの網の接続点では、パケットが転送されてきた第一の網で使用されている前記カプセル化ヘッダ内の前記優先度クラスの情報からパケットが転送されていく第二の網で使用されている前記カプセル化ヘッダ内の優先度クラスの領域にマッピングを行うことを特徴とする請求項 8 に記載の VPN 構成方式。

【請求項 1 5】

可変長パケットにより通信を行うユーザに対してパケット通信サービスを提供するための第一の通信網と、

同様に可変長パケットにより通信を行うユーザに対してパケット通信サービスを提供するための第一の通信網があり、

前記第一の通信網では、特定のユーザのパケットを他のユーザのパケットと混合させない閉域網を構成するために、前記通信網の内部では可変長パケットに対して網内を転送するために特別に付与する第一のカプセルヘッダを網の入りで付与し、網の出口で削除する構成を持ち、

前記第二の通信網でも同様に、特定のユーザのパケットを他のユーザのパケットと混合させない閉域網を構成するために、前記通信網の内部では可変長パケットに対して網内を転送するために特別に付与する第二のカプセルヘッダを網の入りで付与し、網の出口で削除する構成を持ち、

双方の網の接続点には双方の網に所属するインターワークルータを配置し、

前記インターワークルータ装置では、第一の通信網から第二の通信網に転送される特定のユーザのパケットに対しては、第一のカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、第二の通信網への方路選択及び第二の通信網で使用する第二のカプセルヘッダを生成し、

第二の通信網から第一の通信網に転送される特定のユーザのパケットに対しては、第二のカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、第一の通信網への方路選択及び第一の通信網で使用する第一のカプセルヘッダを生成することにより、

第一の網及び第二の網にまたがる閉域網を構成することを特徴とする、可変長

パケット通信によるVPN (Virtual Private Network) 構成方式。

【請求項16】

可変長パケットにより通信を行うユーザに対してパケット通信サービスを提供するための第一の通信網と、

同様に可変長パケットにより通信を行うユーザに対してパケット通信サービスを提供するための第一の通信網があり、

前記第一の通信網では、特定のユーザのパケットを他のユーザのパケットと混合させない閉域網を構成するために、前記通信網の内部では可変長パケットに対して網内を転送するために特別に付与する第一のカプセルヘッダを網の入り口で付与し、網の出口で削除する構成を持ち、

前記第二の通信網でも同様に、特定のユーザのパケットを他のユーザのパケットと混合させない閉域網を構成するために、前記通信網の内部では可変長パケットに対して網内を転送するために特別に付与する第二のカプセルヘッダを網の入り口で付与し、網の出口で削除する構成を持ち、

双方の網の接続点は、それぞれインターワークルータを配置して前記両インターワークルータを接続する形式をとり、両インターワークルータ間では他網との接続を行う特定のユーザのパケットを他のユーザのパケットと分離するためにインターワークカプセルヘッダを使用して転送することとし、

第一の網から第二の網に送られるパケットに関しては、

第一の網の前記インターワークルータ装置では、第一の通信網から第二の通信網に転送される特定のユーザのパケットに対しては、第一のカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、第二の通信網への方路選択及び前記インターワークカプセルヘッダを生成して第二の網のインターワークルータ装置に転送し、

第二の網のインターワークルータ装置ではインターワークカプセルヘッダ及び可変長パケットのヘッダ情報より第二の通信網への方路選択及び第二の通信網で使用する第二のカプセルヘッダを生成し、

第二の網から第一の網に送られるパケットに関しては、

第二の網の前記インターワークルータ装置では、第二の通信網から第一の通信

網に転送される特定のユーザのパケットに対しては、第二のカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、第一の通信網への方路選択及び前記インターワークカプセルヘッダを生成して第一の網のインターワークルータ装置に転送し、

第一の網のインターワークルータ装置ではインターワークカプセルヘッダ及び可変長パケットのヘッダ情報より第一の通信網への方路選択及び第一の通信網で使用する第一のカプセルヘッダを生成することにより、

第一の網及び第二の網にまたがる閉域網を構成することを特徴とする、可変長パケット通信によるVPN (Virtual Private Network) 構成方式。

【請求項 17】

可変長パケットにより通信を行うユーザに対してパケット通信サービスを提供するための第一の通信網と、

同様に可変長パケットにより通信を行うユーザに対してパケット通信サービスを提供するための第一の通信網があり、

前記第一の通信網では、特定のユーザのパケットを他のユーザのパケットと混合させない閉域網を構成するために、前記通信網の内部では可変長パケットに対して網内を転送するために特別に付与する第一のカプセルヘッダを網の入り口で付与し、網の出口で削除する構成を持ち、

前記第二の通信網でも同様に、特定のユーザのパケットを他のユーザのパケットと混合させない閉域網を構成するために、前記通信網の内部では可変長パケットに対して網内を転送するために特別に付与する第二のカプセルヘッダを網の入り口で付与し、網の出口で削除する構成を持ち、

双方の網の接続点は、それぞれインターワークルータを配置して前記両インターワークルータを可変長パケットを識別するIXを介して接続する形式をとり、両インターワークルータ間では他網との接続を行う特定のユーザのパケットを他のユーザのパケットと分離するためにインターワークカプセルヘッダを使用して転送することとし、

第一の網から第二の網に送られるパケットに関しては、

第一の網の前記インターワークルータ装置では、第一の通信網から第二の通信

網に転送される特定のユーザのパケットに対しては、第一のカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、IXの通信網への方路選択及び前記インターワークカプセルヘッダを生成してIXに転送し、

IXではインターワークカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、第二の通信網への方路選択及び前記インターワークカプセルヘッダを生成して第二のインターワークルータに転送し、

第二の網のインターワークルータ装置ではインターワークカプセルヘッダ及び可変長パケットのヘッダ情報より第二の通信網への方路選択及び第二の通信網で使用する第二のカプセルヘッダを生成し、

第二の通信網から第一の通信網に転送される特定のユーザのパケットに対しては、第二のカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、第一の通信網への方路選択及び前記インターワークカプセルヘッダを生成してIXに転送し、

IXではインターワークカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、第一の通信網への方路選択及び前記インターワークカプセルヘッダを生成して第一の網のインターワークルータ装置に転送し、

第一の網のインターワークルータ装置ではインターワークカプセルヘッダ及び可変長パケットのヘッダ情報より第一の通信網への方路選択及び第一の通信網で使用する第一のカプセルヘッダを生成することにより、

第一の網及び第二の網にまたがる閉域網を構成することを特徴とする、可変長パケット通信によるVPN (Virtual Private Network) 構成方式。

【請求項18】

可変長パケットにより通信を行うユーザに対してパケット通信サービスを提供するための第一の通信網と、

同様に可変長パケットにより通信を行うユーザに対してパケット通信サービスを提供するための第一の通信網があり、

前記第一の通信網では、特定のユーザのパケットを他のユーザのパケットと混合させない閉域網を構成するために、前記通信網の内部では可変長パケットに対して網内を転送するために特別に付与する第一のカプセルヘッダを網の入り口で

付与し、網の出口で削除する構成を持ち、

前記第二の通信網でも同様に、特定のユーザのパケットを他のユーザのパケットと混合させない閉域網を構成するために、前記通信網の内部では可変長パケットに対して網内を転送するために特別に付与する第二のカプセルヘッダを網の入り口で付与し、網の出口で削除する構成を持ち、

双方の網の接続点は、それぞれインターワークルータを配置して前記両インターワークルータを可変長パケットを識別しないで下位レイヤにより転送を行うIXを介して接続する形式をとり、両インターワークルータ間では他網との接続を行う特定のユーザのパケットを他のユーザのパケットと分離するためにインターワークカプセルヘッダを使用して転送することとし、

第一の網から第二の網に送られるパケットに関しては、

第一の網の前記インターワークルータ装置では、第一の通信網から第二の通信網に転送される特定のユーザのパケットに対しては、第一のカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、IXの通信網への方路選択及び前記インターワークカプセルヘッダを生成してIXに転送し、

IXではインターワークカプセルヘッダにより、第二の通信網への方路選択及び前記インターワークカプセルヘッダを生成して第二のインターワークルータに転送し、

第二の網のインターワークルータ装置ではインターワークカプセルヘッダ及び可変長パケットのヘッダ情報より第二の通信網への方路選択及び第二の通信網で使用する第二のカプセルヘッダを生成し、

第二の通信網から第一の通信網に転送される特定のユーザのパケットに対しては、第二のカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、第一の通信網への方路選択及び前記インターワークカプセルヘッダを生成してIXに転送し、

IXではインターワークカプセルヘッダにより、第一の通信網への方路選択及び前記インターワークカプセルヘッダを生成して第一の網のインターワークルータ装置に転送し、

第一の網のインターワークルータ装置ではインターワークカプセルヘッダ及び

可変長パケットのヘッダ情報より第一の通信網への方路選択及び第一の通信網で使用する第一のカプセルヘッダを生成することにより、

第一の網及び第二の網にまたがる閉域網を構成することを特徴とする、可変長パケット通信によるVPN (Virtual Private Network) 構成方式。

【請求項 19】

複数のネットワークに接続される伝送路を収容し、各伝送路から到来する可変長パケットを所望のネットワークに出力する機能を持ち、

前記複数のネットワークのうち少なくとも2つのネットワークは、前記ネットワークの内部で使用するカプセルヘッダを用いて可変長パケットをカプセル化して転送を行うカプセル化ネットワークであり、

第一のカプセル化ネットワークからカプセル化された可変長パケットが到来し、第二のカプセル化ネットワークへパケットが転送される場合には、第一のネットワークにおけるカプセルヘッダと可変長パケットヘッダの組み合わせにより第二のネットワークへの出力伝送路及び第二のネットワーク内で使用されるカプセル化ヘッダを生成し、第一のネットワークで使用されるカプセル化ヘッダを削除し、第二のネットワークで使用されるカプセル化ヘッダを付与して第二のネットワークに出力することを特徴とするインターワークルータ装置。

【請求項 20】

前記可変長パケットがインターネットプロトコルパケットであることを特徴とする請求項 19 記載のインターワークルータ装置。

【請求項 21】

前記第一のカプセル化ネットワークのカプセル化プロトコルと前記第二のカプセル化ネットワークのカプセル化プロトコルが異なるカプセル化プロトコルを採用していることを特徴とする請求項 19 記載のインターワークルータ装置。

【請求項 22】

第一の網または第二の網のカプセル化ヘッダとして、インターネットプロトコルによるカプセルヘッダを用いることを特徴とした請求項 19 記載のインターワークルータ装置。

【請求項 2 3】

第一の網または第二の網のカプセル化ヘッダとして、インターネットプロトコルの下位レイヤにあたる、A T M通信方式のヘッダを使用することを特徴とした請求項 1 9 記載のインターワークルータ装置。

【請求項 2 4】

第一の網または第二の網のカプセル化ヘッダとして、インターネットプロトコルの下位レイヤにあたる、H D L C（P P P、フレームリレー）通信方式のヘッダを使用することを特徴とした請求項 1 9 記載のインターワークルータ装置。

【請求項 2 5】

第一の網または第二の網のカプセル化ヘッダとして、インターネットプロトコルの下位レイヤにあたる、M P L S（Multi-Protocol Layer Switching）通信方式のヘッダを使用することを特徴とした請求項 1 9 記載のインターワークルータ装置。

【請求項 2 6】

それぞれの網において使用されるカプセル化ヘッダ内にパケット転送の優先度クラスを持ち、2つの網の接続点では、パケットが転送されてきた第一の網で使用されている前記カプセル化ヘッダ内の前記優先度クラスの情報からパケットが転送されていく第二の網で使用されている前記カプセル化ヘッダ内の優先度クラスの領域にマッピングを行うことを特徴とする請求項 1 9 記載のインターワークルータ装置。

【請求項 2 7】

前記各伝送路は下位レイヤ処理部に收容されパケットレイヤ処理部を介してコアスイッチと接続する構成を持ち、前記下位レイヤ処理部では到来した可変長パケットのカプセルヘッダの解析を行い、装置内部で使用する装置内入力V P N番号をカプセルヘッダから生成し、装置内V P N番号と可変長パケットをパケットレイヤ処理部に転送する機能を持ち、パケットレイヤ処理部では装置内入力V P N番号と可変長パケットのヘッダ領域の情報から出力方路番号及び装置内出力カプセル番号を生成し、コアスイッチでは出力方路番号に応じて所望の伝送路に接続されるパケットレイヤ処理部を選択して装置内出力カプセル番号及びパケット

レイヤ処理部を介してパケットを下位レイヤ処理部に転送し、下位レイヤ処理部では装置内出力カプセル番号より出力する網で使用するカプセルヘッダに変換することによりカプセル化を行うことを特徴とする請求項 19 記載のインターワークルータ装置。

【請求項 28】

前記装置内入力VPN番号及び装置内出力VPN番号にQoSを識別するフィールドを設け、入力側の網のカプセル化ヘッダから前記入力VPN番号のQoSフィールドにマッピングを行い、前記パケットレイヤ処理部では入力VPN番号のQoSフィールドの値から出力側VPN番号のQoSフィールドにマッピングを行い、出力側下位レイヤ処理部では出力側VPN番号のQoSフィールドの値から出力側カプセル化ヘッダのQoSに相当するフィールドにマッピングを行うことにより、第一のネットワークのQoS情報を第二のネットワークのQoS情報に伝達することを特徴とした請求項 19 記載のインターワークルータ装置。

【請求項 29】

第一のネットワークのカプセル化プロトコルにはATMヘッダを用い、第二のネットワークのカプセル化プロトコルにはIPカプセル化を用い、第一のネットワークから到来した可変長パケットのATMヘッダに付与されているCLPビットの値を請求項 28 に記載した方法で第二のネットワーク側のIPカプセルヘッダのTOSフィールドにマッピングし、第二ネットワークから到来した可変長パケットのIPカプセルヘッダに付与されているTOSの値を請求項 28 に記載した方法で第一のネットワーク側のATMヘッダのCLPフィールドにマッピングすることを特徴とする請求項 28 記載のインターワークルータ装置。

【請求項 30】

前記可変長パケットにはIPパケットを用い、入力するカプセル化プロトコルより固定長の入力VPN番号を生成し、入力VPN番号及びIPパケットのヘッダ領域の組み合わせにより出力方路番号及び固定長の出力VPN番号を生成し、出力側で前記VPN番号からカプセル化ヘッダを生成することを特徴とする請求項 19 記載のインターワークルータ装置。

【請求項 3 1】

ひとつのネットワークに接続される伝送路を収容し、各伝送路から到来する可変長パケットを所望のネットワークに出力する機能を持ち、

前記ひとつのネットワークでは、前記ネットワークの内部で使用するカプセルヘッダを用いて可変長パケットをカプセル化して転送を行うカプセル化ネットワークであり、

カプセル化された可変長パケットが到来し、所望の方路にパケットが転送される場合には、入力側カプセルヘッダと可変長パケットヘッダの組み合わせにより出力側伝送路及び出力側で使用するカプセル化ヘッダを生成し、入力側で使用するカプセル化ヘッダを削除し、出力側で使用するカプセル化ヘッダを付与して第二のネットワークに出力することを特徴とするインターワークルータ装置。

【請求項 3 2】

複数のネットワークに接続される伝送路を収容し、各伝送路から到来する可変長パケットを所望のネットワークに出力する機能を持ち、

前記複数のネットワークのうち少なくとも2つのネットワークは、前記ネットワークの内部で使用するカプセルヘッダを用いて可変長パケットをカプセル化して転送を行うカプセル化ネットワークであり、

第一のカプセル化ネットワークからカプセル化された可変長パケットが到来し、第二のカプセル化ネットワークへパケットが転送される場合には、第一のネットワークにおけるカプセルヘッダと可変長パケットヘッダの組み合わせにより第二のネットワークへの出力伝送路及び第二のネットワーク内で使用されるカプセル化ヘッダを生成し、第一のネットワークで使用するカプセル化ヘッダを削除し、第二のネットワークで使用するカプセル化ヘッダを付与して第二のネットワークに出力することによりカプセル化プロトコルを変換する機能を持つことを特徴とするインターワークルータ装置。

【請求項 3 3】

第1の通信網の入り口で、上記第1の通信網で閉域網を構成するために使用される第1のカプセルヘッダが付与された、宛先情報を含むヘッダを有するパケッ

トを受信し、上記パケットを第2の通信網に送信するパケット通信方法であって、

上記第1のカプセルヘッダが付与された上記パケットを受信すると、上記ヘッダと上記第1のカプセルヘッダとから、上記第2の通信網で閉域網を構成するために使用される第2のカプセルヘッダを生成し、

上記第1のカプセルヘッダが付与された上記パケットから上記第1のカプセルヘッダを除去し、

上記パケットに上記第2のカプセルヘッダを付与することを特徴とするパケット通信方法。

【請求項34】

上記ヘッダと上記第1のカプセルヘッダとを用いて方路検索を行うことを特徴とする請求項33に記載のパケット通信方法。

【請求項35】

第1の通信網の入り口で、上記第1の通信網で閉域網を構成するために使用される第1のカプセルヘッダが付与された、宛先情報を含むヘッダを有するパケットを受信し、上記パケットを第2の通信網に送信するパケット通信方法であって、
上記第1のカプセルヘッダが付与された上記パケットを受信すると、上記ヘッダと上記第1のカプセルヘッダとから、上記第2の通信網で閉域網を構成するために使用される第2のカプセルヘッダ生成するのに必要なインデックスを生成し、
上記第1のカプセルヘッダが付与された上記パケットから上記第1のカプセルヘッダを除去し、

上記第2のカプセルヘッダ生成するのに必要なインデックスに基づき上記パケットに上記第2のカプセルヘッダを付与することを特徴とするパケット通信方法。

【請求項36】

上記ヘッダと上記第2のカプセルヘッダ生成するのに必要なインデックスとを用いて方路検索を行うことを特徴とする請求項35に記載のパケット通信方法。

【請求項37】

前記パケットは、IP（インターネットプロトコル）パケットであることを特

徴とする請求項 3 3 乃至請求項 3 6 の何れかに記載の packets 通信方法。

【請求項 3 8】

前記第 1 のカプセルヘッダ及び第 2 のカプセルヘッダは、インターネットプロトコルによるカプセルヘッダを用いることを特徴とする請求項 3 7 に記載の packets 通信方法。

【請求項 3 9】

その中で閉域網を構成するために、宛先情報を含むヘッダが付加されたデータに第 1 のカプセルヘッダを付与する第 1 の通信網と、その中で閉域網を構成するために、宛先情報を含むヘッダが付加されたデータに第 2 のカプセルヘッダを付与する第 2 の通信網とを相互に接続する通信装置であって、

上記第 1 の通信網から送信された上記第 1 のカプセルヘッダが付与されたデータを受信したとき、上記ヘッダと上記第 1 のカプセルヘッダとによりルート検索を行い、上記ヘッダと上記第 1 のカプセルヘッダとから上記第 2 のカプセルヘッダを生成し、上記第 1 のカプセルヘッダを除去する一方で上記生成した第 2 のカプセルヘッダを付与する受信処理部と、

上記受信処理部に接続され、上記ルート検索の結果に応じた方路に、上記第 2 のカプセルヘッダが付与されたデータを送信するスイッチとを有することを特徴とする通信装置。

【請求項 4 0】

上記スイッチに接続され、上記スイッチから上記第 2 のカプセルヘッダが付与されたデータが送信され、そのデータを上記第 2 の通信網に送信する送信処理部を有することを特徴とする請求項 3 9 に記載の通信装置。

【請求項 4 1】

その中で閉域網を構成するために、IP (Internet Protocol) packets に第 1 のカプセルヘッダを付与して通信を行う第 1 の通信網と、その中で閉域網を構成するために、IP packets に第 2 のカプセルヘッダを付与して通信を行う第 2 の通信網とを相互に接続する packets 中継装置であって、

上記第 1 の通信網から送信された上記第 1 のカプセルヘッダが付与された IP packets を受信したとき、上記 IP packets 内の IP ヘッダと上記第 1 のカプセル

ルヘッダとにより上記第2のカプセルヘッダを生成するカプセルヘッダ生成手段と、

上記カプセルヘッダ作成手段と接続され、上記第1の通信網から送信された上記第1のカプセルヘッダが付与されたIPパケットを受信すると、上記第1のカプセルヘッダを除去すると共に上記第1のカプセルヘッダが除去されたIPパケットに上記カプセルヘッダ生成手段で生成された第2のカプセルヘッダを付加する手段とを有することを特徴とするパケット中継装置。

【請求項42】

上記カプセルヘッダ生成手段は、上記IPパケット内のIPヘッダと上記第1のカプセルヘッダとによりインデックスを生成する手段と、上記インデックスを生成する手段で生成されたインデックスに応じて上記第2のカプセルヘッダを生成する手段とを有することを特徴とする請求項41に記載のパケット中継装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明はインターネットにおける仮想専用網（VPN：Virtual Private Network）構築方法及びインターネットサービスプロバイダ間を接続するインターワークルータに関する。

【0002】

【従来の技術】

インターネット・プロトコル（Internet protocol：IP）ネットワーク上では、電子メール、WWW（World Wide Web）などのアプリケーションを使用することができる。また、IPネットワークは、従来の電話ベースの交換網と比較して構築コストが安い。そのためインターネットは近年爆発的に普及している。このような状況の下、IPで構築した企業内網（イントラネット）は、企業活動にも欠かすことの出来ないものとなってきている。

【0003】

企業は複数の地域に偏在している場合が多い。この場合、各地域の企業網を相互接続し、一つの企業網を構築する必要がある。企業網を複数地域にわたって

構築する場合、次の2つの方法が考えられる。

【0004】

第1は、各地域の企業内網を専用線で相互接続することである。このように構築することにより、企業網を外部のネットワークから隔絶、セキュリティを確保を確保することができる。

【0005】

第2に、IPsec (IP security protocol) 技術により、自網のネットワークの packets を識別する機能を端末に設け、インターネット内ではグローバルアドレスに基づくIP packets として転送を行うことである。悪意のユーザからの攻撃にはこの識別機能と、暗号化により対抗することでVPNを実現することができる。

【0006】

しかし、専用線を使用するとネットワークコストが上昇してしまうこと、さらにIPsec方式によるVPNでは、アタック及び暗号解読により悪意のユーザの侵入を許したり、暗号化処理が高速ネットワークの速度のボトルネックになったり、端末コストが上昇するという問題があった。

【0007】

このため、インターネットが普及し、インターネットが廉価で使えるようになるに従い、網が提供するIPの下位レイヤの機能を用い、インターネット上に仮想的に専用網を構築し、コストを押さえ、かつ外部のネットワークから隔絶した安全な、かつ何らかの品質保証行い要求が高まってきた。

【0008】

この要求を満たすネットワークとして次のようなVPNが考えられている。VPNを提供するインターネット・サービス・プロバイダ (Internet Service Provider: ISP) のネットワークの入り口でカプセル化を行う。ISPのネットワーク上では、このカプセル化したヘッダに基づき転送を行い、ネットワークの出口でカプセルヘッダを外す。このVPN構成方式では、VPN固有のカプセル化ヘッダを用いることにより外部のネットワークから隔絶し、セキュリティを確保している。また、このカプセル化の具体的なプロトコルとしては、IPカプセル化、

MPOA (Multi Protocol over ATM)、MPLS (Multi Protocol Layer Switching) 等の方式があり、1999年2月現在、ITU-T SG13やIETFなどの標準化団体で検討が行われている。また、ITU-T SG13では、網の内部をE.164アドレスによりカプセル化して転送する、Core Protocol (別称GMN-CL) についての検討も行われている。

【0009】

NTT R&D vol.47 No.4 1998 (平成10年4月10日発行) は、GMN-CLにおけるユーザ網とコア網のインターワークを行うアクセス系・エッジノードの構成法を提案している。

【0010】

【発明が解決しようとする課題】

近年の企業活動は広範囲に渡っている。このため、例えば、日、米、欧に拠点を持ち、それぞれの拠点でイントラネットを構築した上で、VPNにより、それらを相互接続したいというニーズが生じてくるものと考えられる。

【0011】

他方、ISPはある特定の地域でサービスを提供しているのが一般的なため、前記したような各拠点のネットワークをVPNにより接続するためには、複数のISPをまたがった形でVPNを構築する必要がある。

【0012】

なお、複数のISPを相互に接続する場合、インターワークのためのゲートウェイを設け、相互接続を行う。このインターワークルータでは、双方のネットワークから到来した相手網行きのパケットをIPヘッダに従って相手網に転送することで、インターワークを実現する。また、日経コミュニケーション1997年12月15日号146頁に記されているように、複数ネットワークの相互インターワークのために、IX (Internet Exchange) と呼ばれる装置を用いて互いのネットワークを接続し、このIXにより、互いの網間で転送されるパケットの転送を行っても良い。このようなIXには、IPパケットを識別して転送を行う「レイヤ3フォワーディング」や、ATM通信装置などで、下位レイヤのヘッダを識別して転送を行う「レイヤ2フォワーディング」を用いる方式がある。

【0013】

本願発明者等は、複数のISPのネットワークをまたがる形でVPNを構成しようとした場合の問題点を検討した。まず、各インターネットサービスプロバイダのネットワークでVPNを構築するために、各ネットワーク内でそれぞれカプセル化を行う。各ネットワークのカプセル化プロトコルは、一般に異なるものとなると考えられる。この場合、インターワークルータでは、双方のネットワークの共通のプロトコルであるIPパケットのIPヘッダ情報を検索して宛先方路を決定し、他網行きのパケットであるか否かを検索する必要がある。

【0014】

しかし、インターワークルータは、IPレイヤより下位レイヤのプロトコルはインターフェースで終端してしまうため、前段の網でVPNを構成するためにつけられているカプセル化ヘッダをはずしてIPアドレスを検索する事により次のホップ情報を決定し、また後段の網でのVPNを構成するためのカプセルヘッダを生成してパケットに付与することになる。したがって、インターワーク装置内部では、VPN内のパケットとVPN以外の網のパケットとが混在してしまう。そのため、悪意のユーザによる不正ヘッダの付与により、インターワークルータを基点としてVPNへの侵入が可能になるという問題がある。

【0015】

また、企業によってはグローバルアドレスを使用せずにインターナルアドレスを用いてVPNを構成することがある。この場合、インターワークルータでカプセル化ヘッダを一旦はずしてしまうと、受信側のISP側では、インターナルアドレスが複数のVPNでそれぞれ独自に使用されているので、同一のアドレスを持つパケットを区別することが出来ない。このため、パケットの転送先が決定できない。複数のISPにまたがって、インターネット上にVPN構成する場合、上述のような問題点がある（第1の課題）。

【0016】

更にそれぞれのISPにおけるサービスは均一でない。例えば通信品質を例に説明すると、あるISPではATMのVCを用いてパスを張ることにより各VPNの品質の保証しており、別のISPではDiffserv(Differentiated Services)

により品質の保証を行っている場合、双方で構成するVPNを相互に接続する場合、エンド・トゥー・エンドで通信品質を規定することは困難である。（第2の課題）。

【0017】

上述のように、実用レベルで、複数のISPにまたがってインターネット上にVPNを構築することは困難である。

【0018】

そこで、本発明は複数のISPにまたがってVPN構築する方法及び、複数のISPにまたがってVPN構築する場合において、それらのISP間を接続するインターワークルータを提供することにある。

【0019】

【課題を解決するための手段】

第1の課題を解決するため、VPN識別番号であるカプセル化ヘッダとIPヘッダ双方の情報を用いて、出力方路の決定及び出力側ISP網内でのカプセル化ヘッダの生成を行う機能をインターワークルータ装置に設ける。下位レイヤにATMを用いるMPLS網を運用するISP同士を接続する場合を例により具体的に説明すると、VPN識別に使用するカプセル化ヘッダであるATMのVPI、VCI等のヘッダ情報と、IPアドレスをキーに検索を行い、次の方路及び次のネットワーク内部でのVPN識別に使用するATMのVPI、VCI等のヘッダ情報を生成し、後段の網に送り出す際に生成したヘッダ情報を付与して送出する。

【0020】

これによりVPNのインターワークが実現でき、複数のISPにまたがる地域に対する、インターネット上でのVPN構成を構成することが出来る。

【0021】

第二の課題を解決するするために、入力側のカプセル化ヘッダ領域のQoSをあらわすフィールドの値を、出力側のカプセル化ヘッダ領域のQoSをあらわすフィールドの値にマッピングを行う。これにより、双方の網の品質情報を透過的に転送することができる。

【0022】

【発明の実施の形態】

以下、図を用いて本発明の実施例について説明する。

【0023】

図1、図2を用いて本発明による複数ISPにまたがる下位レイヤにより分離されたVPNの構成法およびそのインターワークルータの役割について説明する。ここで下位レイヤとは、IPパケットをカプセル化するプロトコルを指し、IPパケットをIPヘッダでカプセル化する場合にも、このカプセルヘッダを下位レイヤのヘッダとして表記することとする。

【0024】

まず、図2により、従来のルータを用いて複数のISPにまたがるVPNを構成した場合の問題点について説明する。図2では、下位レイヤでカプセル化することによりVPNを実現するISP1(2-1)とISP2(2-2)が既存ルータ(9)によりインターワークしている。ISP1はA地区でサービスを展開しており、LAN1(1-1)、LAN2(1-2)、LANa(1-a)を収容している。ISP2はB地区でサービスを展開しており、LAN3(1-3)、LAN4(1-4)、LANb(1-b)を収容している。また、LAN1、LAN2、LAN3、LAN4は同一会社のLANであり、VPNを構成したいと考えている。またLANa、LANbも同一会社のLANであり、VPNを構成したいと考えている。このような場合、同一ISP内においては、網の入り口と網の入り口にカプセルチャネルを張ることにより、他のユーザのパケットと分離することができるため、セキュリティの高いネットワークを構築できる。しかし、ISP1とISP2にわたってVPNを設定しようとする場合、既存ルータでは入力側のインターフェース部で下位レイヤを終端し、IPレベルでマージしてからパケットフォワーでリング処理を行うため、IPレベルで複数のユーザのパケットが混じってしまう問題がある。すなわち、VPN内のパケットとそれ以外のパケットが混じってしまう。従って、悪意のユーザがIPアドレスを偽って網に侵入することも可能となる。さらに二つの会社がプライベートアドレスを用いて社内LANを構築しようとした場合には、それぞれの会社では独立にアドレス

をアサインするため、同一のIPアドレスをアサインすることがある。この場合、既存ルータではアドレスのバッティングのため、正しくパケットを転送することができない。

【0025】

次に図1を用いて、本発明による前記問題の解決法について説明する。例えば会社AのLAN1から会社AのLAN3に通信する場合を説明する。本実施例ではISP1はIPカプセル化によりVPNを実現しており、ISP2はMPLS（ATMによる）によりカプセル化を行いVPNを実現している。LAN1から到来したパケットはISP1（2-1）に入るとISP1はIPカプセル化を行い、パケットはIPカプセル化論理チャネル（5-1）通じてインターワークルータに到着する。インターワークルータ（9）ではパケットが搭載されてきたIPカプセル化論理チャネルを示すIPカプセル化ヘッダと、元々のパケットヘッダの双方から出力方路を検索すると共に、ISP2内でのカプセル化ヘッダを作成する。本実施例ではISP2はMPLSでサービスを行っているので、ATMのヘッダを作成する。ATMによりカプセル化されたパケットは、ATM論理チャネル（5-3）を通り、LAN3に送られる。インターワークルータでは、カプセルヘッダ及びIPヘッダで検索を行っているので、会社Aと会社Bがそれぞれプライベートアドレスを用いて、IPアドレスがバッティングする場合にもそれぞれ正しいあて先に転送することが可能となる。

【0026】

本実施例ではカプセル化プロトコルとして、IPレイヤのカプセル化方式であるIPカプセル化と、ATMを用いてカプセル化を行う方式説明した。もちろんフレームリレーやHDLC系のプロトコルを用いてカプセル化を行ってもよい。

【0027】

図3では本発明による、複数ISPにまたがるVPN構成法の1実施例について、網構成とプロトコルスタックを用いて説明する。ここではカプセル化プロトコルは限定していない。ISP1（2-1）はエッジノード（3-1，3-2）を介してそれぞれLAN1（1-1）、LAN2（1-2）を収容している。同様にISP2（2-2）はエッジノード（3-3，3-4）を介してそれぞれL

AN 3 (1-3)、LAN 4 (1-4)をはじめとする複数の網を収容している。またそれぞれのISPは自網の入り口から出口にかけて、IPパケットを網内で使用するヘッダでカプセル化して転送を行っている。そしてカプセルヘッダをVPNに固有に割り当てることにより、VPNトラフィックを網内の別のトラフィックから識別してVPNに関する閉域網を構成している。ISP 1 (2-1)とISP 2 (2-2)はインターワークルータ (10)により互いにインターワークしており、相手網行きのトラフィックはインターワークルータを介して相手網に転送される。

【0028】

例えばLAN 1とLAN 3を結ぶVPN (VPN 1と呼ぶ事とする)を構成する場合について説明すると、LAN 1から送出されたLAN 3宛のIPパケットはエッジノード (3-1)においてIPアドレスにより検索され、まずVPN 1に属すインターワークルータ宛のパケットと認識され、VPN 1のインターワークルータ (10)行きのカプセルヘッダ (レイヤ図中103a)が付与され、インターワークルータ (10)に到達する。インターワークルータ (10)はカプセルヘッダ (レイヤ図中103a)とIPアドレスにより検索され、VPN 1に属すエッジノード (3-3)宛のパケットであることを検索し、ISP 2内でVPN 1でエッジノード (3-3)宛のカプセルヘッダ (レイヤ図中103b)を付与し、ISP 2内をカプセルヘッダに従いエッジノード (3-3)に転送される。エッジノード (3-3)ではカプセルヘッダを外し、LAN 3にIPパケットを転送する。これにより、両網内にまたがるVPNのIPパケットを他トラフィックと混合されることなく転送することが出来る。

【0029】

なお、グローバルアドレスを用いたIPパケットについては、下位レイヤ情報に依存させず、ひとまとめにして転送先および(カプセルヘッダを使用する場合には)カプセルヘッダを決定することにより、従来の網内と同様に転送を行うことが出来る。

【0030】

インターワークルータ (10)の動作を図4、図5、図6を用いて説明する。

図4は従来のルータ装置の処理フローであり、図5、図6は本発明によるインターワークルータ（10）の処理フローである。従来のルータでは、パケットが到着すると、ISP1（2-1）での転送に用いられる物理レイヤを終端（201）し、ISP1内の転送に使用したカプセルヘッダを除去（202）してから、IPヘッダの値により方路検索を行い（203）、スイッチを介して所望方路に転送する（204）。その後、ISP2での転送に用いられるカプセルヘッダを付与（205）し、その後物理レイヤの処理を行って（206）伝送路から送出する。このフローでは、ISP1のカプセルヘッダを除去して、IPヘッダのみで方路を決定するため、複数VPNのトラフィックが一旦マージされてしまう。本発明のインターワークルータによれば、そのような問題を回避できる。

【0031】

図3は、本発明のインターワークルータ（10）が実行するアルゴリズムである。パケットが到着すると、ISP1（2-1）での転送に用いられる物理レイヤを終端（211）し、ISP1内の転送に使用したカプセルヘッダとIPヘッダの値により方路検索およびISP2内のカプセル化ヘッダの生成を行う（212）。その後ISP1カプセルヘッダを除去（213）し、ISP2での転送に用いられるカプセルヘッダを付与（214）し、スイッチに送信する。そして、スイッチにより、所望の方路に転送（215）される。その後物理レイヤの処理を行って（216）伝送路から送出する。これにより、別の網のトラフィックと分離することができる。また、スイッチに、カプセルヘッダが除去された裸のIPパケットが流れることがないので、この部分から他人がVPNに挿入することは出来ない。すなわち、ISP2内で使用される内部ヘッダが付加されていないIPパケットが紛れ込み、そのパケットがISP2内のVPNに流れ込むということはない。従って、安全性も高くなる。

【0032】

また別の実施例として図6を説明する。本実施例のインターワークルータは、ISP1内の転送に使用したカプセルヘッダとIPヘッダの値の組と、カプセルヘッダインデックスとの対応テーブルと、カプセルヘッダインデックスとISP2内の転送に使用したカプセルヘッダとの対応テーブルを有している。パケット

が到着すると、ISP1 (2-1) での転送に用いられる物理レイヤを終端 (221) し、ISP1 内の転送に使用したカプセルヘッダとIPヘッダの値により方路検索とカプセルヘッダインデックスの生成を行う (222)。その後、上記IPパケットISP1カプセルヘッダを除去 (223) し、その除去されたIPパケットに、生成したカプセルヘッダインデックスを付与してスイッチに送信し、スイッチにより所望の方路に転送される (224)。そして、カプセルヘッダIndexからISP2での転送に用いられるカプセルヘッダを生成、付与 (225) する。その後物理レイヤの処理を行って (226) 伝送路から送出する。この構成によっても、図5の場合と同様に、安全性の高い閉域網を構成することが出来る。すなわち、カプセルヘッダIndexが付与されていないIPパケットが紛れ込むことはない。

【0033】

次に図7～図10を用いて、MPLSによりVPNをサポートするISP1とIPカプセルを用いてVPNをサポートするISP2にまたがるVPNの実現方式とパケット構成例を説明する。

【0034】

図7は網構成とプロトコルスタックを示している。図3ではカプセル化方式を特定せずに説明したが、図7は、ISP1はMPLS、ISP2はIPカプセル化を採用した場合の例を示している。インターワークルータ (10) では、図3と同様にカプセル化ヘッダに相当するATMレイヤ (104a) 及びIPレイヤ (101)、IPカプセルレイヤ (104b) 及びIPレイヤ (101) の組み合わせによりフォワーディングを行う。これにより、VPNがそれぞれプライベートアドレスを用いるためアドレスが重複する場合であっても、正しくフォワーディングすることが可能となる。

【0035】

図8により、IPパケットをATMでカプセル化する方式を説明する。本カプセル化はIETFのRFC1483で標準化されている方式である。IPヘッダ (250) 及びIPペイロード (251) からなるIPパケットにLLC/SNAP (253) を付与し、AAL5ヘッダ (252) 及びAAL5トレイラ (2

55) を付与してAAL5フレームを構成する。PAD(254)はAAL5フレームをATMセルのペイロード(257)長である48オクテットの定数倍にするために挿入する。そしてこのAAL5トレイラを48オクテット毎に分割し、ATMヘッダ(256)を付与し、1乃至複数のATMセルとして転送を行う。

【0036】

図9はRFC791で示されるIPv4パケットフォーマットを示している。IPカプセル化を行う際、カプセル化を行うプロトコルはIPv4ヘッダをそのまま使用し、網内のルータは既存のIPv4ルータを使用することができる。

【0037】

図10はIPトンネルによるカプセル化方式を示している。ユーザの送信したIPヘッダ(260)及びIPペイロード(261)から構成されるIPパケットをカプセル化ヘッダ(264)でカプセル化しており、このカプセル化ヘッダはIPヘッダ(262)とトンネルヘッダ(263)から構成される。このカプセル化ヘッダはISP2内で用いられるもので、網内で一意に識別が可能である。したがって、ユーザがプライベートアドレスを用いた場合でも、網内ではカプセルヘッダによりルーティングを行い、パケットを所望のエッジまで運ぶことができる。本例ではRFC1583によるトンネルヘッダの例を示したが、他にIPカプセル化にはGREカプセル化(RFC1792)やIPモバイルなどがある。

【0038】

インターネットルータ(10)では、図8や図10で示したカプセルヘッダとユーザのIPアドレスを組み合わせ、フォワーディング処理を行うことにより、安全なVPNをISPにまたがり構成することができ、さらにユーザはプライベートアドレスを用いてVPNを構築することができる。

【0039】

図11乃至図19を用いて、インターネットルータ(10)の一実施例について説明する。

【0040】

図1 1はインターワークルータ（10）の1構成例である。制御部（50）は装置全体の制御及び他ノードとのルーティング処理などを行っている。コアスイッチ（51）は各パケットレイヤ処理部（52）間のパケットの転送を行うスイッチである。下位レイヤ処理部（ATM）（53）はISP1のMPLS網を収容するインターフェースであり、下位レイヤ処理部（IPカプセル）（54）はISP2のIPカプセル網を収容するインターフェースである。パケットレイヤ処理部（52）は下位レイヤ処理部（53，54）から下位レイヤの情報及びIPパケットを受け取り、下位レイヤの情報とIPパケットのヘッダ情報の組み合わせによりパケットの転送先を決定する。

【0041】

まず受信方向の処理の流れから説明する。図1 2に下位レイヤ処理部（ATM）（53）のブロック構成を示す。ISP1の網から到来した信号はまず物理レイヤ処理部（150）にて物理レイヤを終端し、ATMレイヤ処理部（151）にてATMレイヤを終端する。この際、再構成されたIPパケットとともに、受信側のVPN識別機能を果たしているATMヘッダも同時にVPN番号付与部（152）に送付する。VPN番号付与部（152）では装置内でVPNの識別に利用するVPN番号をATMヘッダより生成する。この際受信側VPN番号テーブル（153）が用いられる。そしてこのVPN番号とIPパケットはパケット処理部IF（154）を介してパケットレイヤ処理部に転送される。

【0042】

図1 3には受信側VPN番号テーブル（153）の構成例を示している。このテーブルでは入力側ATMヘッダ（300）と入力側VPN番号（303）のペアから構成されており、入力側ATMヘッダが入力キーとなって入力側VPN番号（303）を出力する。入力キーとなる入力側ATMヘッダとしては、VPI／VCI（301）の他、パケットの転送優先度を示すCLP（Cell of Priority）ビット（302）をキーとしてもよい。そして装置内で汎用的に使用される入力側VPN番号は装置内VPN番号（304）の他にQoS（Quality of Service）を示すフィールド（305）を設けてもよい。またCLPとQoSのマッ

ピングを行うテーブルをVPN識別のための本テーブルと独立に設けてもよい。

【0043】

図14に下位レイヤ処理部（IPカプセル）（54）の実施例を示す。ISP2から到来した信号は物理レイヤ処理部（170）にて物理レイヤを終端し、次にカプセルレイヤ受信処理部（171）にてカプセルヘッダの終端を行う。この際終端したカプセルヘッダをIPパケットと共にVPN番号付与部（172）へ送付する。VPN番号付与部（172）では装置内でVPNの識別に利用するVPN番号をATMヘッダより生成する。この際受信側VPN番号テーブル（173）が用いられる。そしてこのVPN番号とIPパケットはパケット処理部IF（154）を介してパケットレイヤ処理部に転送される。

【0044】

図15には受信側VPN番号テーブル（173）の構成例を示している。このテーブルは、入力側カプセルヘッダ（310）と入力側VPN番号（303）のペアから構成されており、入力側ATMヘッダが入力キーとなって入力側VPN番号（303）を出力する。入力キーとなる入力側IPカプセルヘッダとしては、カプセルヘッダのソースアドレス（311）の他、パケットの転送優先度を示すTOS（Type of Service）フィールド（302）をキーとしてもよい。そして装置内で汎用的に使用される入力側VPN番号は装置内VPN番号（304）の他にQoSを示すフィールド（305）を設けてもよい。

【0045】

またTOSとQoSのマッピングを行うテーブルをVPN識別のための本テーブルと独立に設けてもよい。

【0046】

図12から図15を用いて説明した方式により、入力側VPN番号（303）とIPパケットがパケットレイヤ処理部（52）に到達した際の処理を図16を用いて説明する。下位レイヤ処理部（180）を介して入力側VPN番号（304）とIPパケットをルート検索・VPN処理部（181）が受け取ると、ここではルート検索・VPNテーブル（182）を用いてIPヘッダ及び入力側VPN番号の双方をキーにしてルート検索及び出力側VPN番号を決定する。これに

より出力方路及び出力側VPN番号とIPパケットは、コアスイッチIFを介してコアスイッチに送付され、所望のパケットレイヤ処理部に到達することとなる。

【0047】

図17にルート検索・VPNテーブルの構成例を示す。入力キーとして入力側VPN番号(320)及びIPヘッダ(323)を用いて検索を行い、出力方路番号(325)及び出力側カプセル番号(326)を出力させる。出力方路番号(326)はコアスイッチ及びその他でパケットを所望のインターフェースに転送するための装置内識別子であり、出力側カプセル番号(326)は出力側の下位レイヤ処理部にてカプセルヘッダを付与するためのカプセルヘッダへの装置内識別子である。出力側カプセル番号(326)にはカプセル番号(327)の他にQoS(328)を設け、優先制御を行ってもよい。

【0048】

次に送信方向の処理について説明する。図16を用いてパケットレイヤ処理部(52)の処理例を示す。コアスイッチIF(184)を介して出力側カプセル番号(326)及びIPパケットを受け取ると、これらの情報を下位レイヤ処理部IFを介して下位レイヤ処理部(53、54)に転送する。

【0049】

図12を用いて、下位レイヤ処理部(ATM)(53)の動作を説明する。下位レイヤ処理部(ATM)(53)ではパケットレイヤ処理部(52)からパケットレイヤ処理部IF(159)を介して出力側カプセル番号(326)及びIPパケットを受信する。次にATMヘッダ決定部(157)はヘッダ生成テーブル(158)を用いてカプセルヘッダに対応するATMヘッダを出力側カプセル番号(326)から生成する。こうして生成されたATMヘッダとIPパケットはATMレイヤ送信処理部(156)でATMセルに変形され、物理レイヤ送信処理部(155)を介してISP1のネットワークへと送信される。

【0050】

図18にヘッダ生成テーブルの構成を示す。出力側カプセル番号をキーとして出力側ATMヘッダを出力する構成となっている。これにより出力側カプセル番

号より出力側ATMヘッダを得ることができる。

【0051】

同様に図14を用いて下位レイヤ処理部（IPカプセル）（54）の動作を説明する。下位レイヤ処理部（IPカプセル）（54）ではパケットレイヤ処理部（52）からパケットレイヤ処理部IF（159）を介して出力側カプセル番号（326）及びIPパケットを受信する。次にカプセルヘッダ決定部（177）はヘッダ生成テーブル（178）を用いてカプセルヘッダに対応するIPカプセルヘッダ及び出力側MACアドレスを出力側カプセル番号（326）から生成する。こうして生成されたIPカプセルヘッダ、出力側MACアドレスとIPパケットはカプセルレイヤ送信処理部（176）でカプセル化処理され、物理レイヤ送信処理部（175）を介してISP1のネットワークへと送信される。

【0052】

図19にヘッダ生成テーブルの構成を示す。出力側カプセル番号をキーとして出力側IPカプセルヘッダ及び出力側MACアドレスを出力する構成となっている。

【0053】

以上インターワークルータ装置の一構成例を示した。本実施例では、入力側、出力側それぞれの処理に内部で統一された入力側VPN番号（320）及び出力側カプセル番号（326）を用いた例を示した。但し、ルート検索・VPNテーブルの入力キーを入力側カプセルヘッダにしてもよいし、出力として直接出力側カプセルヘッダを生成してもよい。

【0054】

また、本実施例で示したテーブルは論理的なテーブルであり、テーブル検索方法として、ツリー構造に代表される検索アルゴリズムを用いてアドレスを出し、所望の出力を得る方式を採用してもよいし、CAMを使った構成や、テーブルを逐次検索していく方式を採用してもよい。

【0055】

図23に本実施例のテーブルの設定のための、NMSから装置に指示を出すインターフェースであり、エージェントが制御部50に搭載される、MIB（Manag

gement Information Base) 構成の一実施例を示す。入力カプセルヘッダEntry (500) は図13に示した受信側VPNテーブルを設定するためのMIBである。同様にVPNクロスコネクトEntry (501) は図17に示したルート検索・VPNテーブル (182) を設定するためのMIBである。同様に出力側カプセルヘッダEntry (502) はヘッダ生成テーブルの1構成例である。これらのMIBに設定された情報は、NMSから制御部 (50) に対して設定され、制御部 (50) がインターワークルータ内各部にテーブル設定する。

【0056】

ここまでにVPNのインターワークについて装置構成を中心に説明してきた。図20から図22を用いて、インターワークルータのネットワーク内での適用例を説明する。

【0057】

図20は2つのISPがそれぞれの所有する2つのインターワークルータを介して接続される例を示す。2つのインターワークルータの間はカプセル化 (103b) によりそれぞれのVPNを識別する構成になっている。そしてそれぞれのインターワークルータ (10a、10b) では、図19までに説明したとおり、カプセルヘッダ (103a、103b、103c) とIPアドレスの組によりルーティング処理を行う。

【0058】

図21は2つのISPがそれぞれの所有するインターワークルータを持ち、レイヤ3処理を行うIXを介して接続される例である。それぞれのインターワークルータとIXの間はカプセル化 (103b) によりそれぞれのVPNを識別する構成になっている。インターワークルータ (10a)、IX (10c) 及びインターワークルータ (10b) では、図19までに説明したとおり、カプセルヘッダ (103a、103b、103c) とIPアドレスの組によりフォワーディング処理を行う。

【0059】

図22は2つのISPはそれぞれのインターワークルータを持ち、2つのISPが、IXを介して接続される例を示す。ここで、IXはレイヤ3処理を行わな

レイヤ2装置で構成されている。この場合もそれぞれのインターワークルータとIXの間はカプセル化(103b)によりそれぞれのVPNを識別する構成になっている。インターワークルータ(10a)とインターワークルータ(10b)では、図19までに説明したとおり、カプセルヘッダ(103a、103b、103c)とIPアドレスの組によりフォワーディング処理を行う。IXはレイヤ2フォワーディングにより転送を行う。

【0060】

なお、本発明では複数ISP間のVPNの接続方式について説明したが、同一ISP内に複数のカプセル化エリアが存在する場合にも、同一のノード構成でVPNを接続することが必要である。その場合でも、本発明で説明した方式により、VPNを接続することができる。

【0061】

【発明の効果】

本発明により複数ISP間にまたがるVPN網を構築することができる。また複数のVPNネットワーク間でQoS情報をインターワークすることができる。

【図面の簡単な説明】

【図1】

本発明によるインターワークルータ動作の概念図である。

【図2】

従来のルータを用いた場合における複数のISP間のインターワーク方式を説明した図である。

【図3】

本発明によるインターワークルータの動作をプロトコルスタックを用いて説明した図である。

【図4】

従来のルータによるISPインターワーク処理方式を説明するフローチャートである。

【図5】

本発明によるインターワークルータの動作を説明するフローチャートである。

【図 6】

本発明によるインターワークルータの動作を説明するフローチャートである。

【図 7】

本発明によるMPLS網とIPカプセル化網の接続形態をプロトコルスタックを用いて説明した図である。

【図 8】

RFC 1483によるIPパケットのATMセル化を説明する図である。

【図 9】

RFC 791によるIPパケットフォーマットを説明する図である。

【図 10】

RFC 1853によるIPトンネルパケットの構成を説明する図である。

【図 11】

本発明によるインターワークルータの1構成例を説明する図である。

【図 12】

本発明によるインターワークルータの下位レイヤ処理部の1構成例を説明する図である。

【図 13】

本発明による下位レイヤ処理部における受信側VPN番号テーブルの構成例を説明する図である。

【図 14】

本発明によるインターワークルータの下位レイヤ処理部の1構成例を説明する図である。

【図 15】

本発明による下位レイヤ処理部における受信側VPN番号テーブルの構成例を説明する図である。

【図 16】

本発明によるインターワークルータのパケットレイヤ処理部の1構成例を説明する図である。

【図 1 7】

本発明によるパケットレイヤ処理部におけるルート検索VPNテーブルの構成例を説明する図である。

【図 1 8】

本発明による下位レイヤ処理部におけるヘッダ生成テーブルの構成例を説明する図である。

【図 1 9】

本発明による下位レイヤ処理部におけるヘッダ生成テーブルの構成例を説明する図である。

【図 2 0】

本発明によるインターワークルータの網内での 1 適用例を説明する図である。

【図 2 1】

本発明によるインターワークルータの網内での 1 適用例を説明する図である。

【図 2 2】

本発明によるインターワークルータの網内での 1 適用例を説明する図である。

【図 2 3】

本実施例のテーブルの設定のための、NMSから装置に指示を出すインターフェースである。

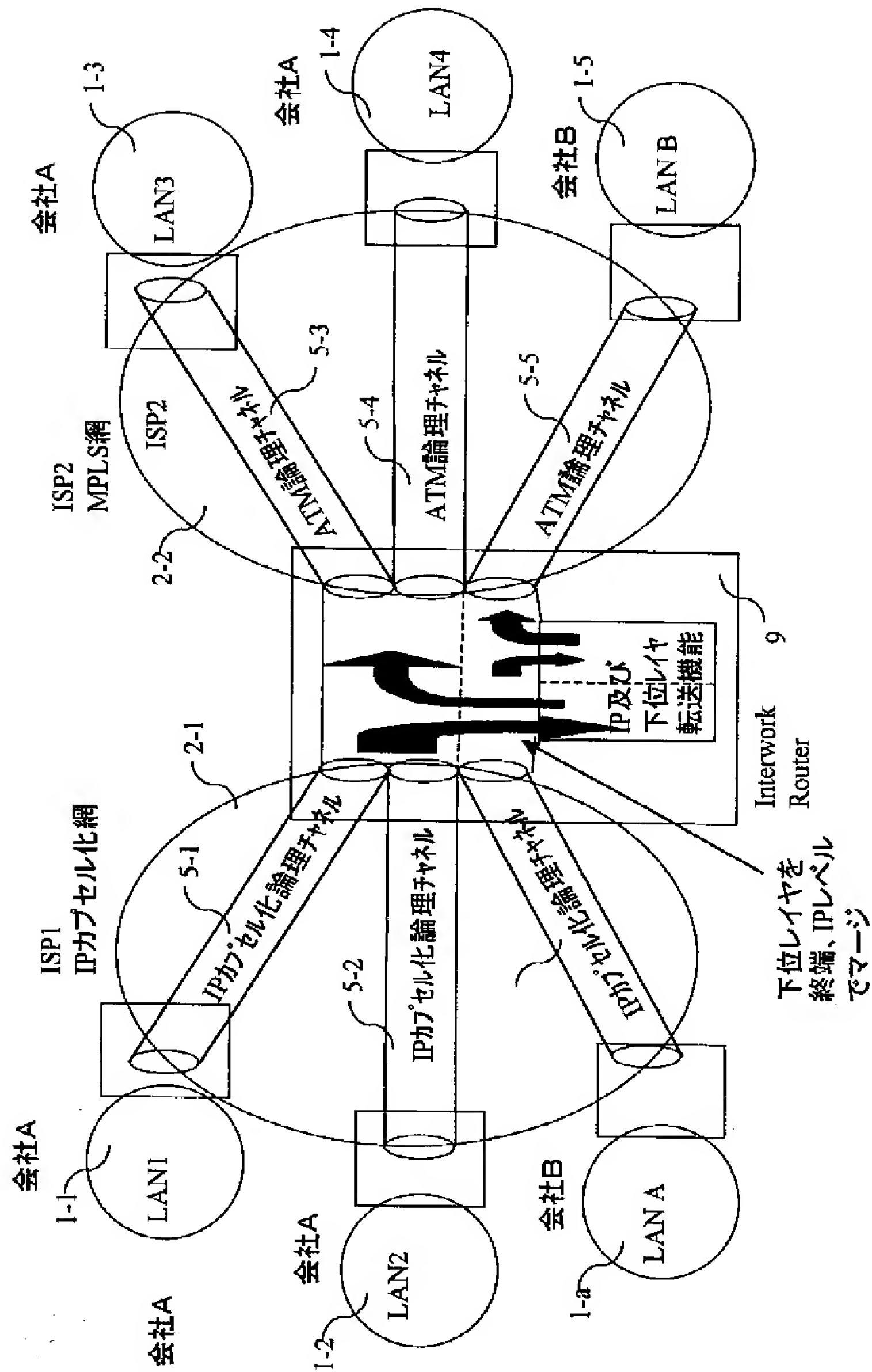
【符号の説明】

2…ISP網、3…エッジノード、10…インターワークルータ装置、50…制御部、51…コアスイッチ、52…パケットレイヤ処理部、53…下位レイヤ処理部（ATM）、54…下位レイヤ処理部（IPカプセル）、152…VPN番号付与部、153…受信側VPN番号テーブル、157…ATMヘッダ決定部、158…ヘッダ生成テーブル、172…VPN番号付与部、173…受信側VPN番号テーブル、177…カプセルヘッダ決定部、178…ヘッダ生成テーブル。

【書類名】 図面

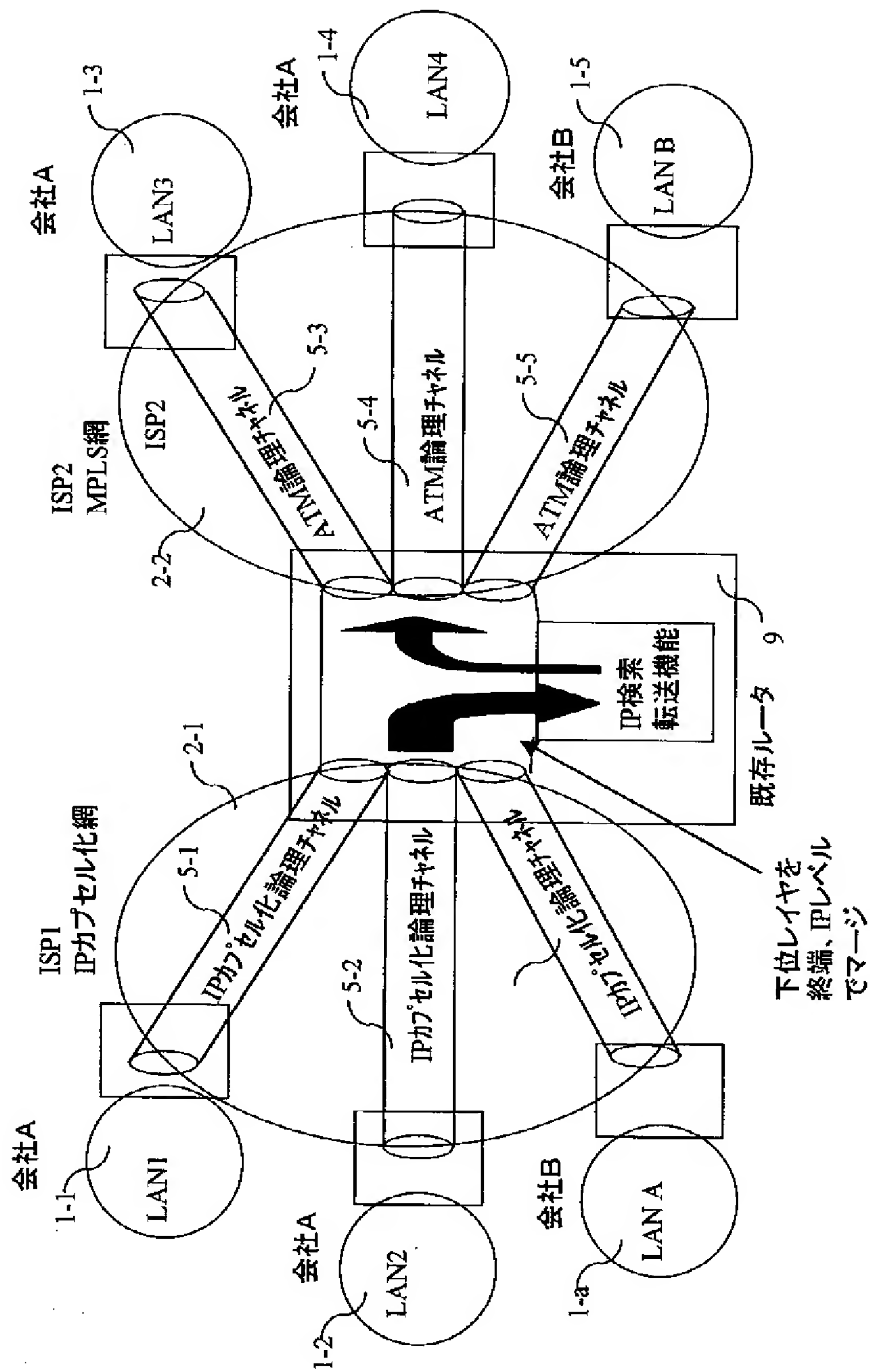
【図 1】

図 1



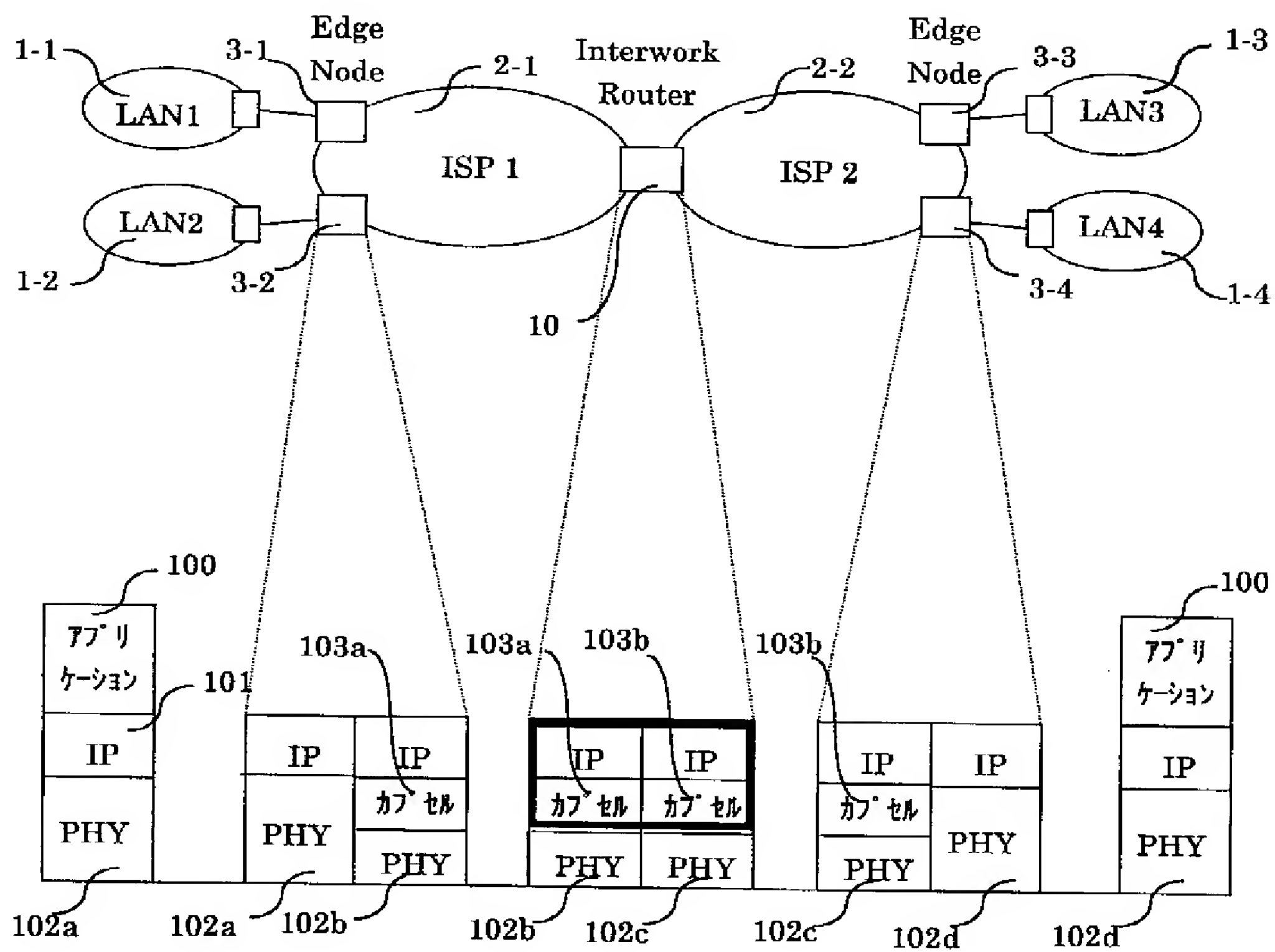
【図2】

図2

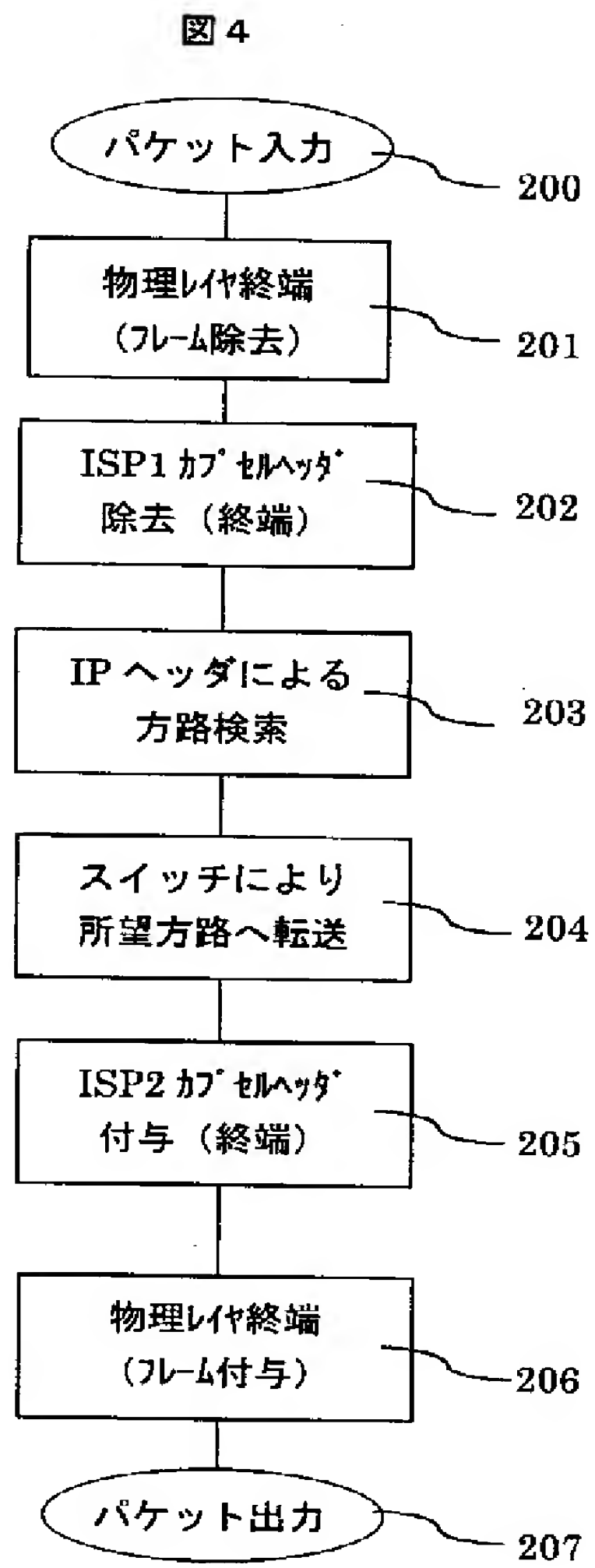


【図3】

図3

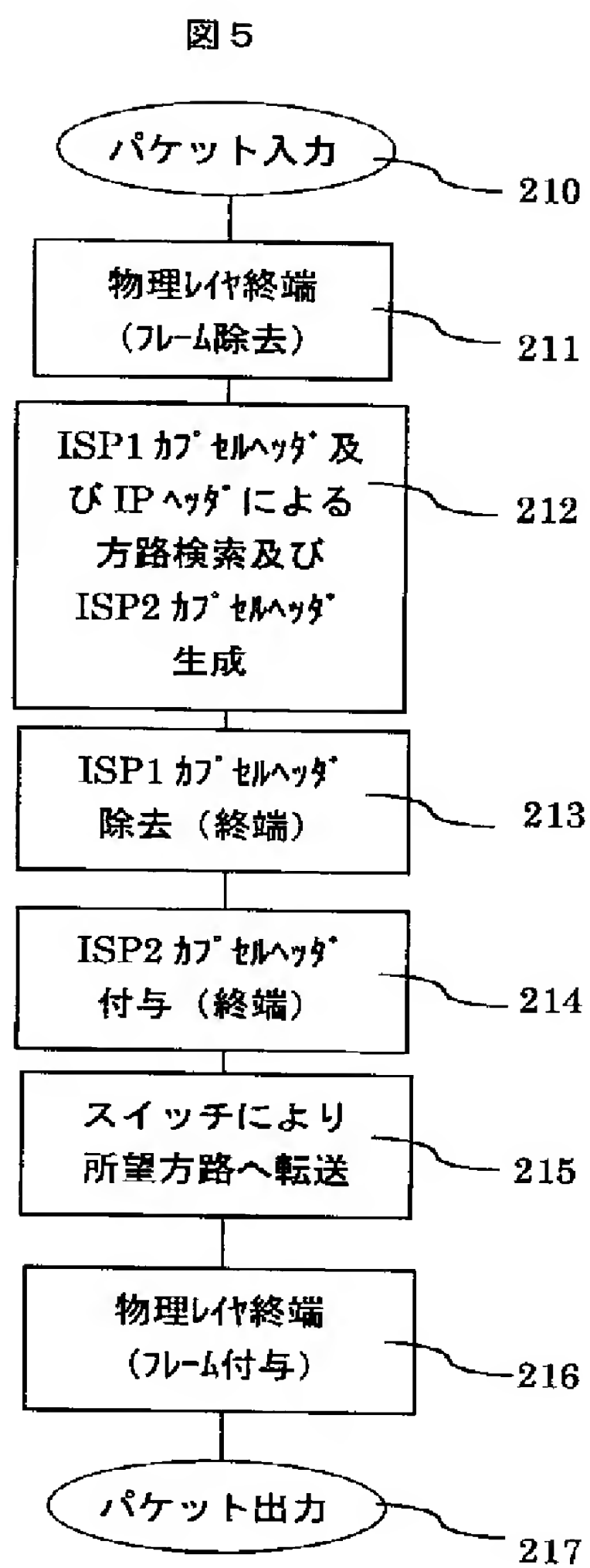


【図4】



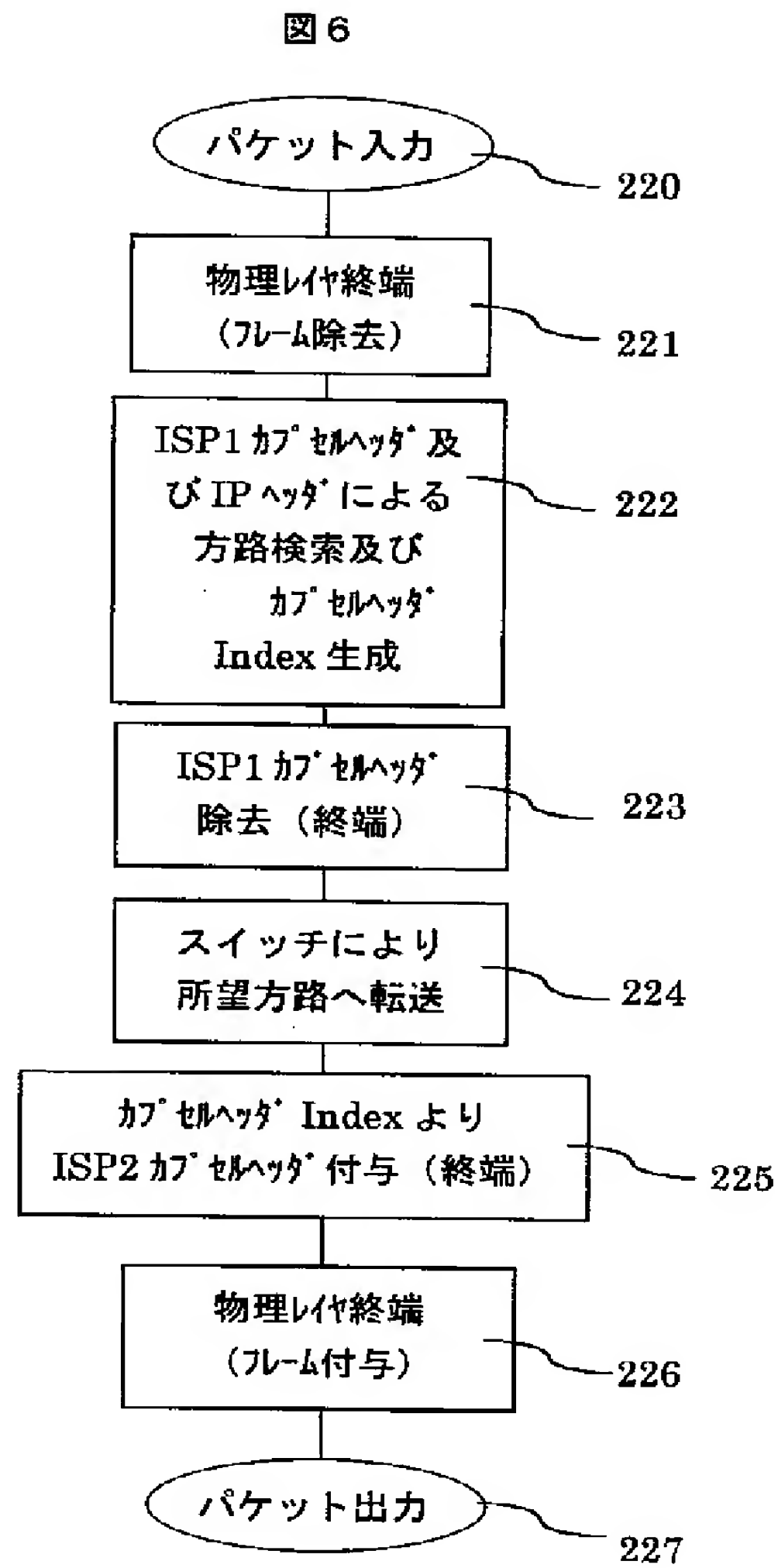
ルータの処理の流れ (従来例)

【図5】



インターワークルータの処理の流れ (本発明)

【図6】



インターワークルータの処理の流れ (本発明)

【図 7】

図 7

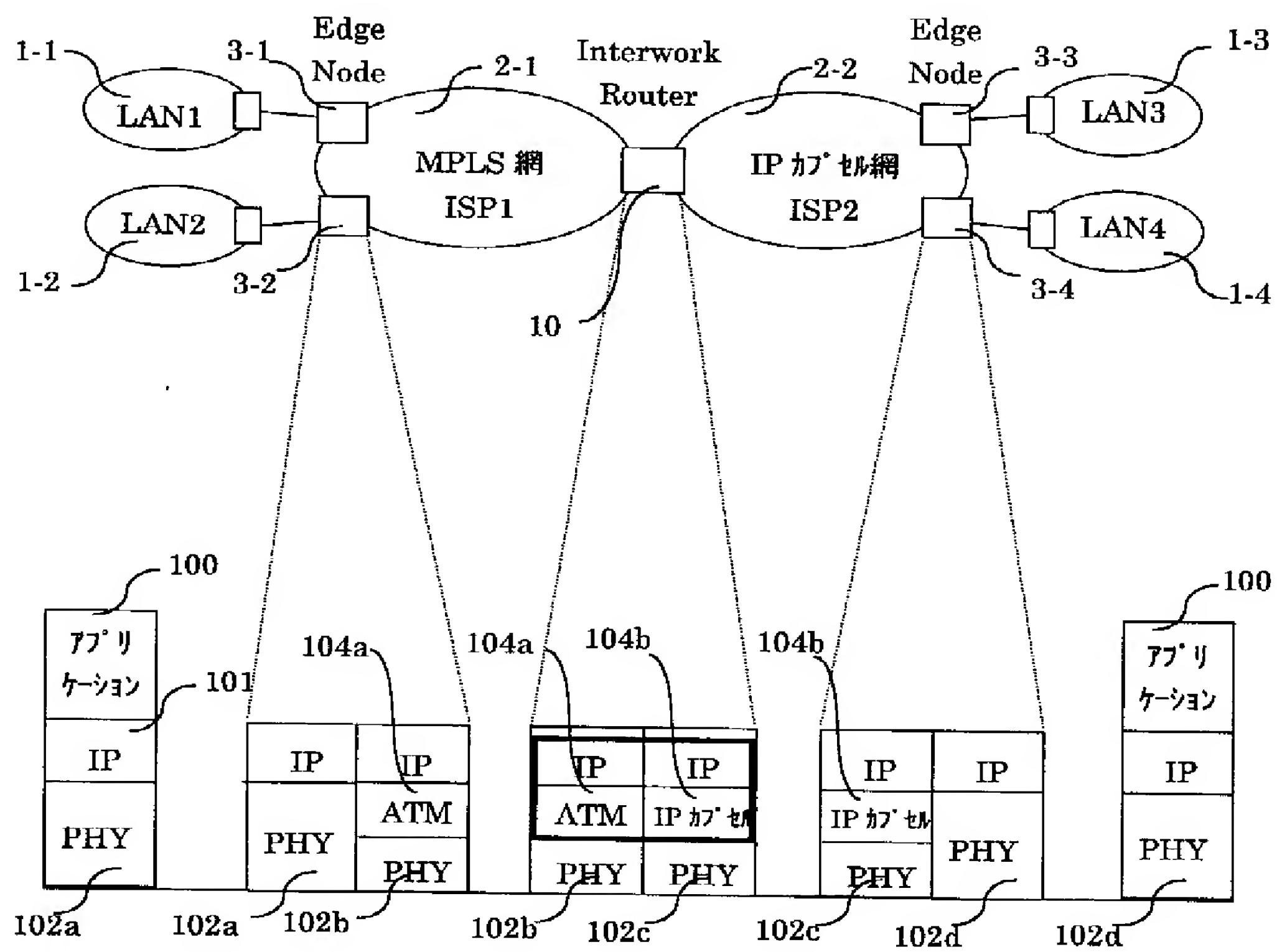
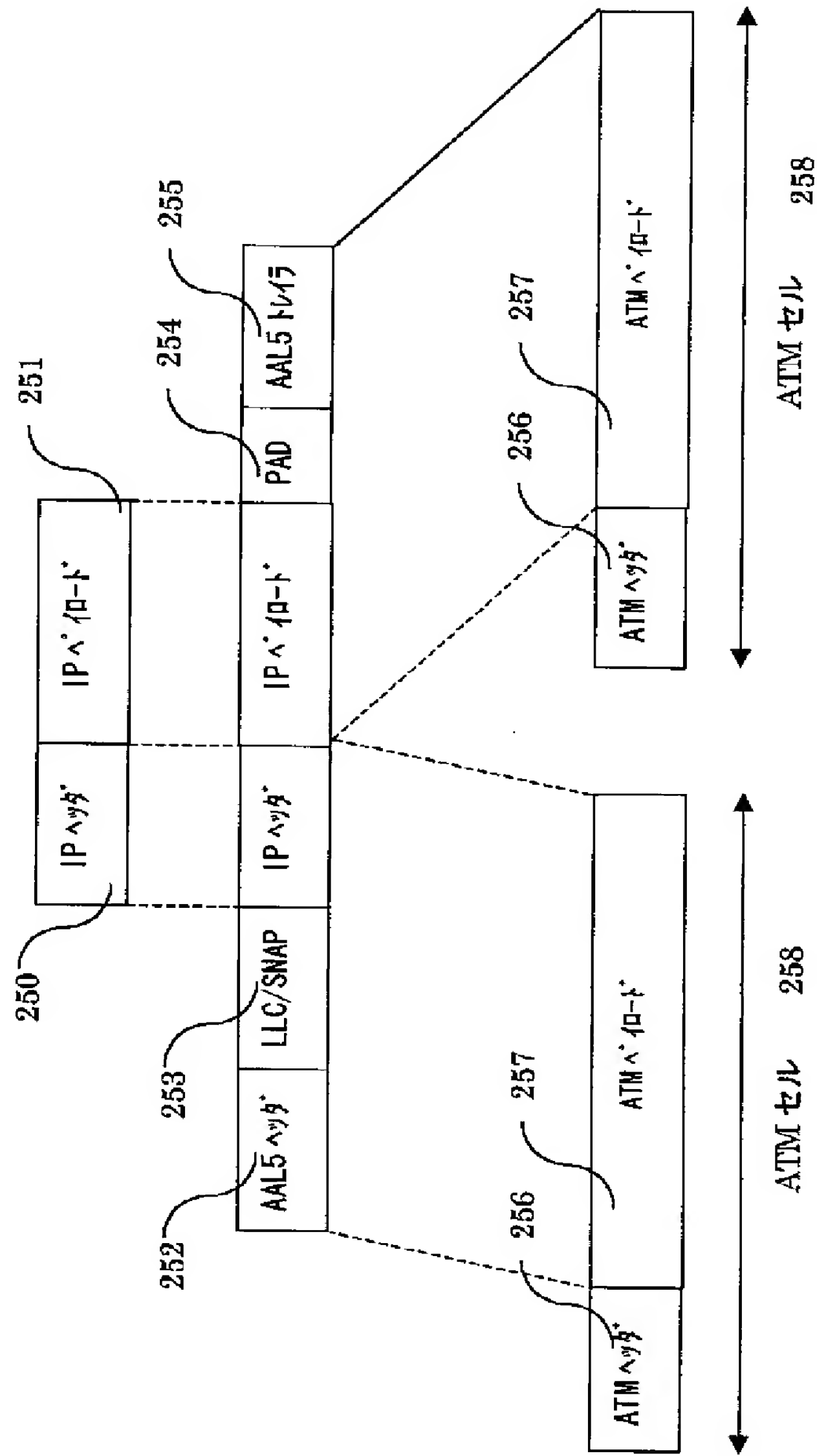


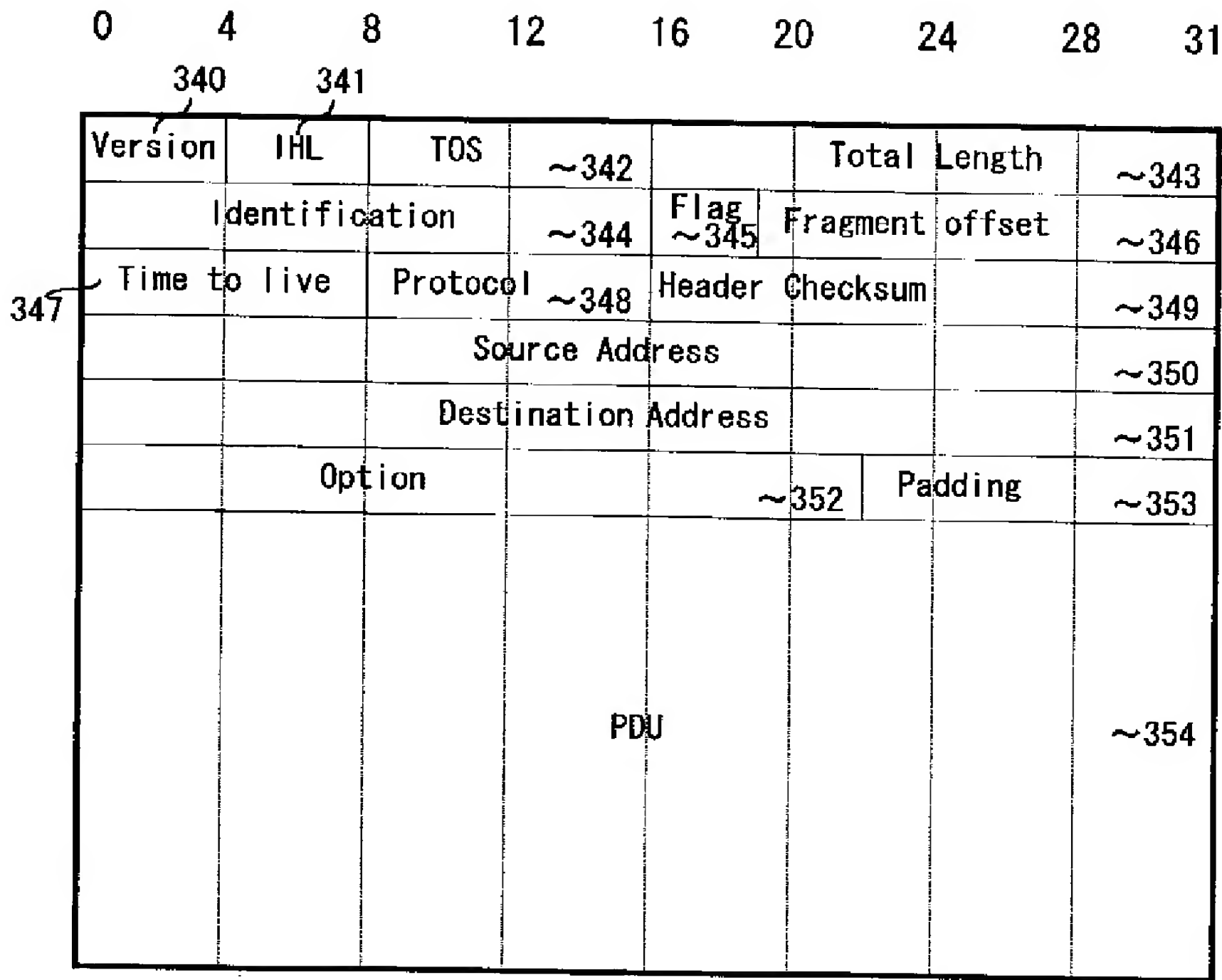
図 8

AAAL5(RFC1483)によるカ⁷セル化



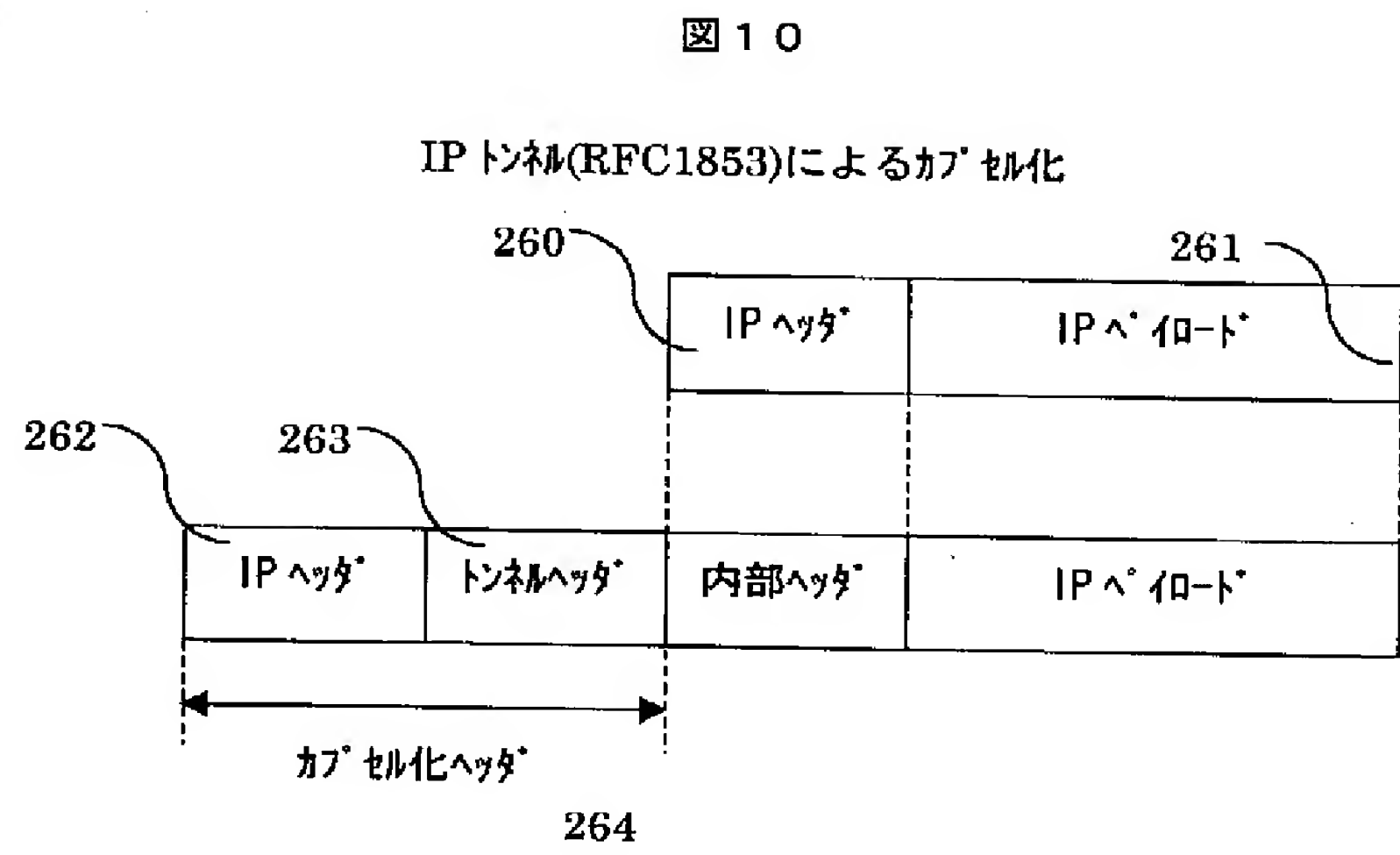
【図 9】

図 9

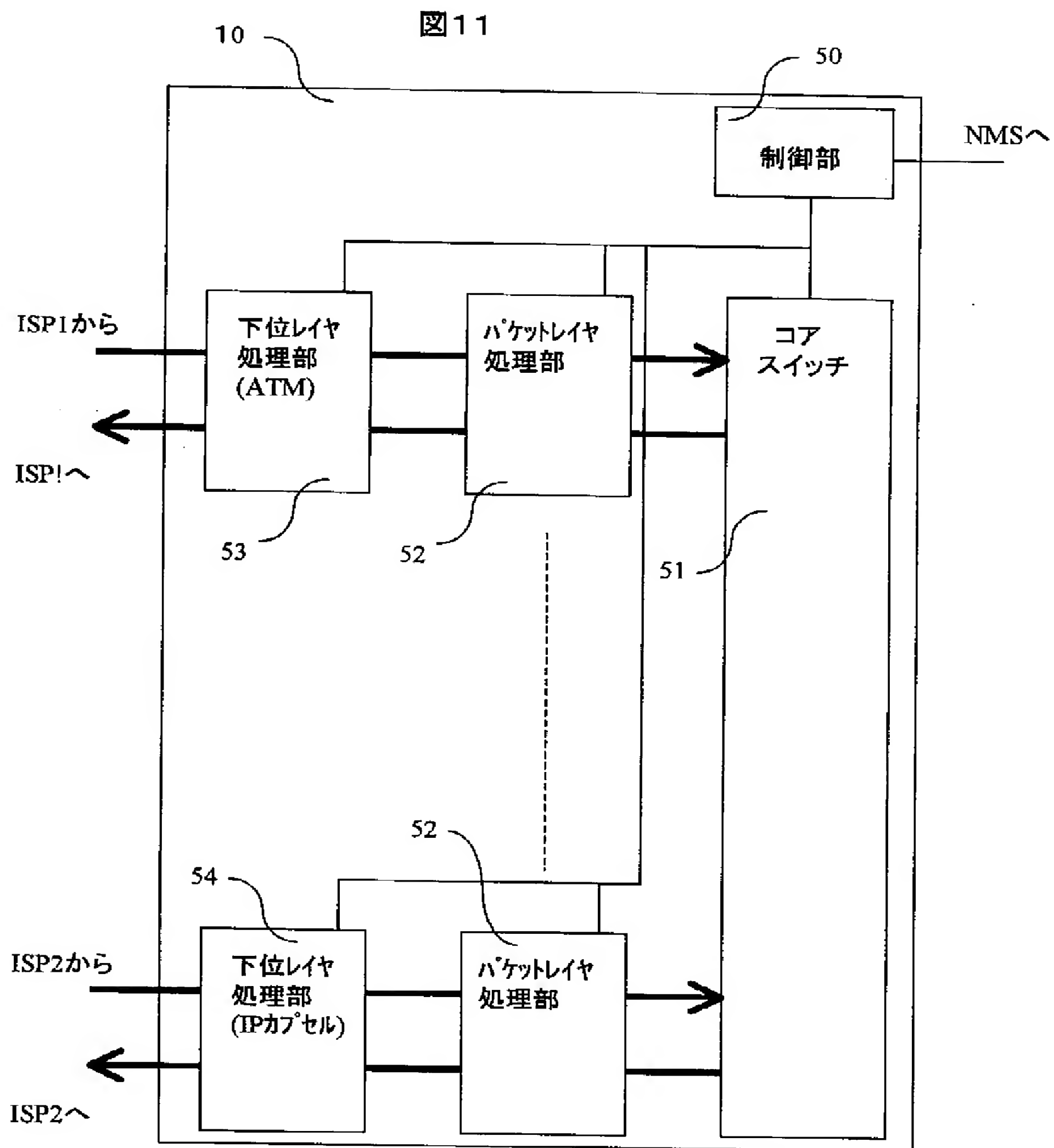


IPv4 フレームフォーマット

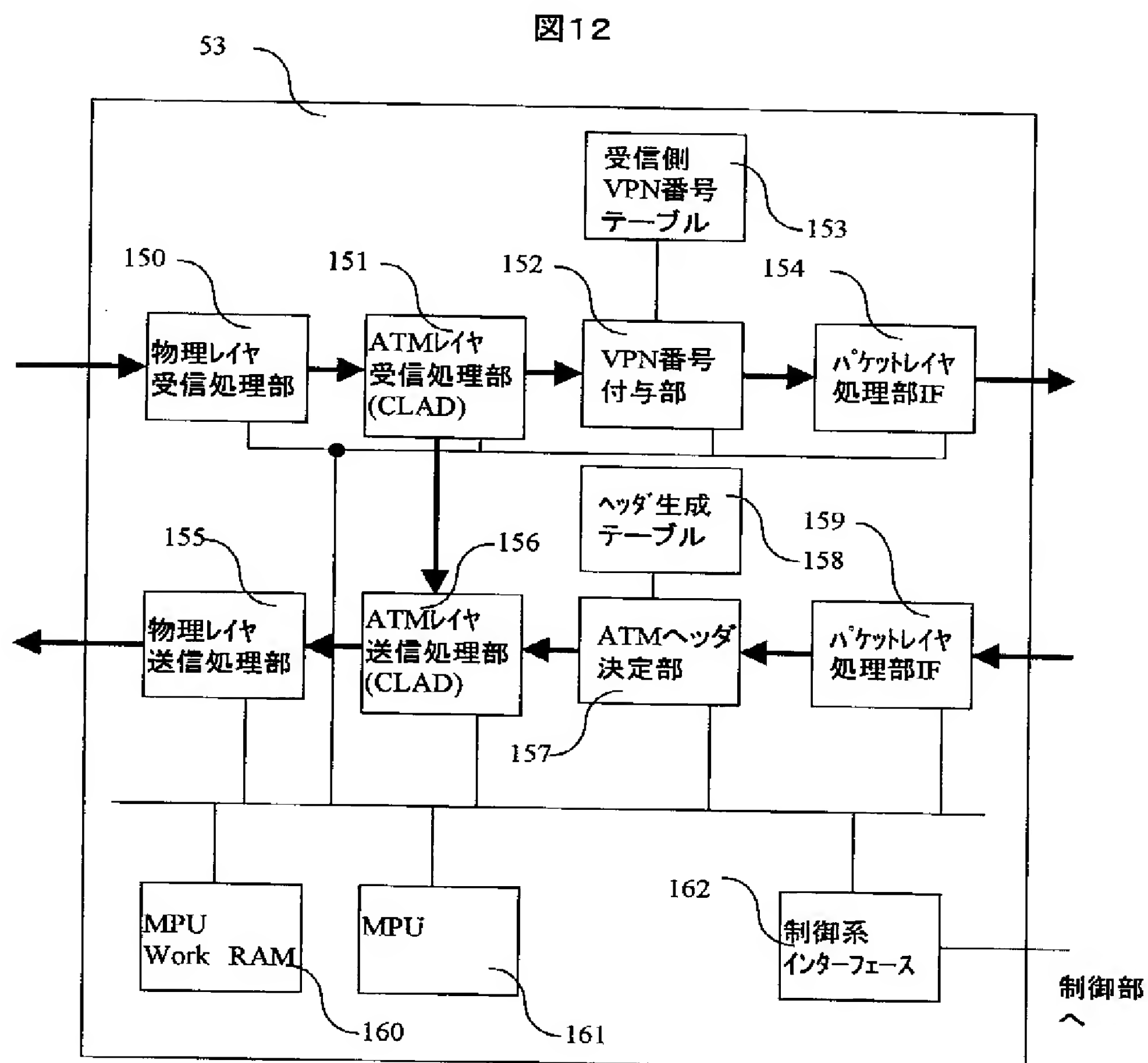
【図 1 0】



【図 1 1】



【図 1 2】

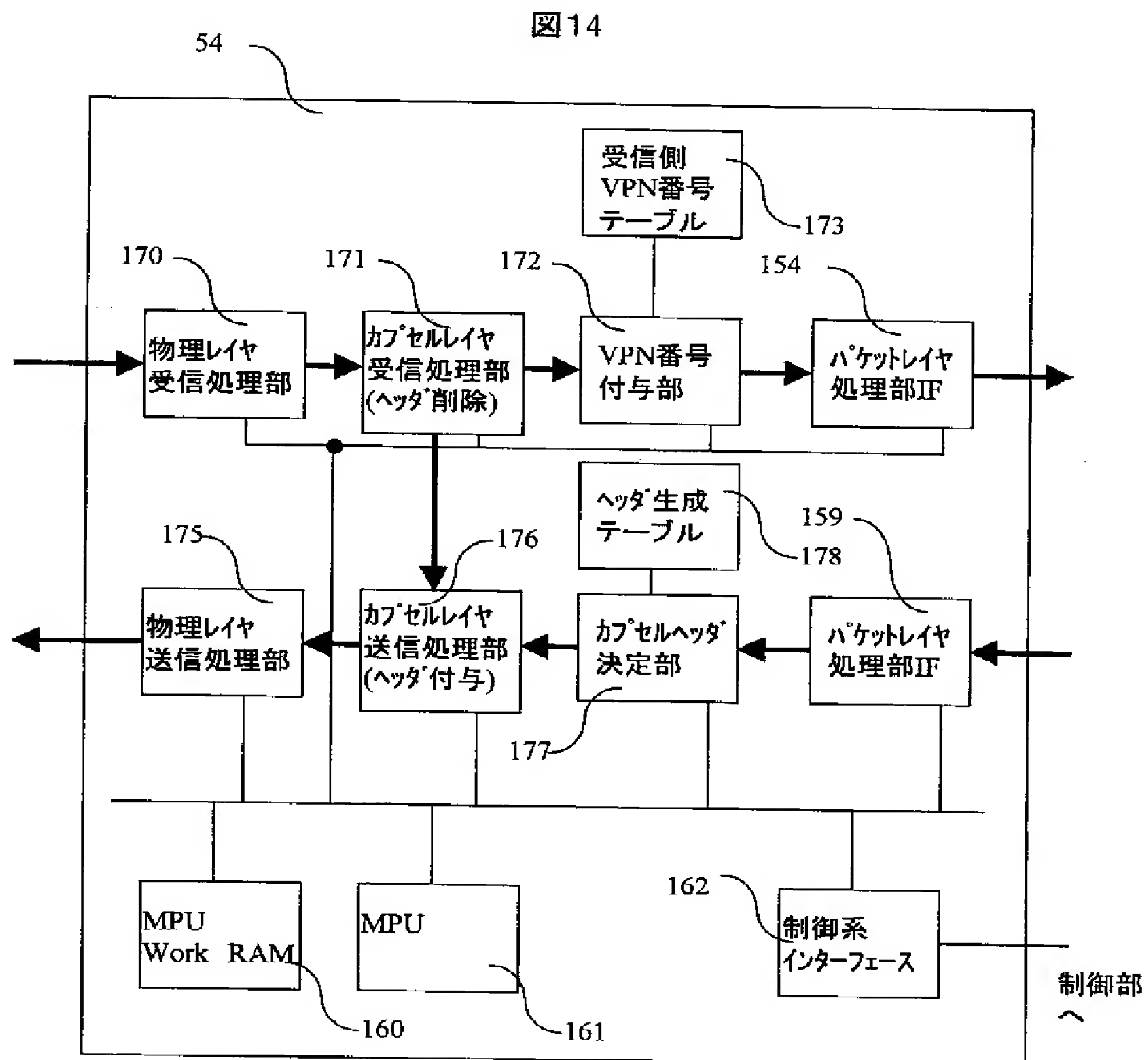


【図 1 3】

図13

| | | | |
|---------------|-----|--------------|---------|
| 300 入力側ATMヘッダ | | 303 入力側VPN番号 | |
| 301 VPI/VC1 | CLP | 装置内VPN番号 | QoS 305 |
| a | 0 | 0 | 0 |
| b | 1 | 12 | 7 |
| 302 | | 304 | |
| m | 0 | 20 | 0 |
| n | 0 | 22 | 0 |
| 入力キー | | 出力キー | |

【図14】

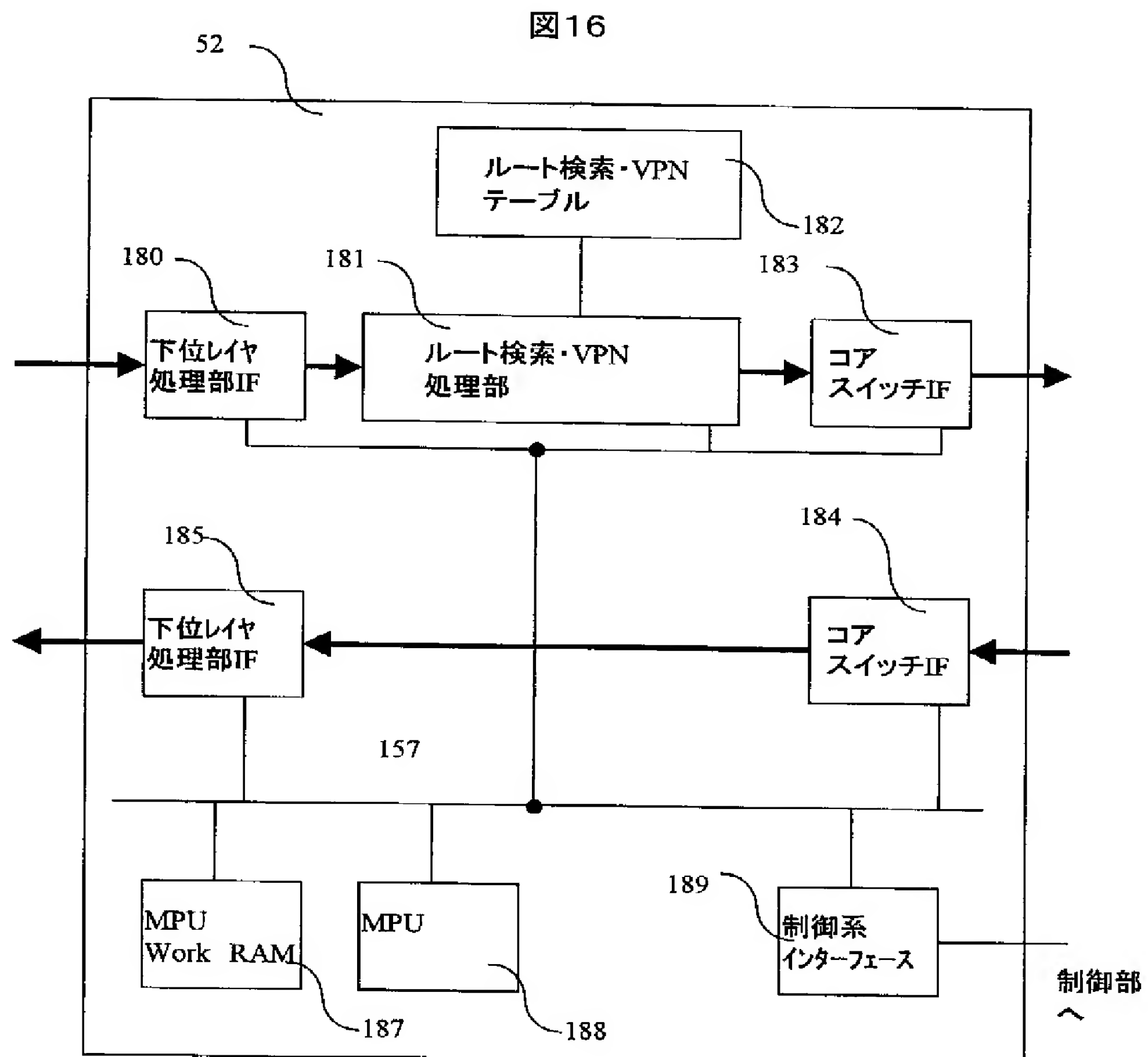


【図 1 5】

図15

| | | | |
|------------------|-----|--------------|---------|
| 310 入力側カプセルヘッダ | | 303 入力側VPN番号 | |
| 311 カプセルヘッダ (SA) | TOS | 装置内VPN番号 | 305 QoS |
| a | 0 | 0 | 0 |
| b | 1 | 12 | 7 |
| 312 | | 304 | |
| m | 0 | 20 | 0 |
| n | 0 | 22 | 0 |
| 入力キー | | 出力キー | |

【図16】



【図 17】

図 17

| | | | | | | |
|----------|---|---------|---------------------|--------|-----------|-----|
| 入力側VPN番号 | | IPヘッダ | | 出力方路番号 | 出力側カプセル番号 | |
| 装置内VPN番号 | | QoS | Destination Address | | カプセル番号 | QoS |
| 1 | 0 | A.a.a.a | 15 | 5 | 0 | |
| 1 | 0 | b.a.a.a | 10 | 7 | 0 | |
| n | | 324 | 327 | 328 | | |
| | | | | | | |
| | | | | | | |
| n | 0 | b.a.a.a | 8 | 13 | 0 | |
| n | 0 | c.a.a.a | 2 | 11 | 0 | |

入力キー

出力キー

【図 1 8】

図18

| 出力側カプセル番号 | | 出力側ATMヘッダ | |
|-----------|-----|-----------|-----|
| 下位レイヤ番号 | QoS | VPI/VCI | CLP |
| 5 | 0 | a | 0 |
| 7 | 0 | b | 1 |
| 331 | 332 | 334 | 335 |
| | | | |
| | | | |
| 13 | 0 | m | 0 |
| 11 | 0 | n | 0 |

← 入力キー

出力キー →

【図 1 9】

図19

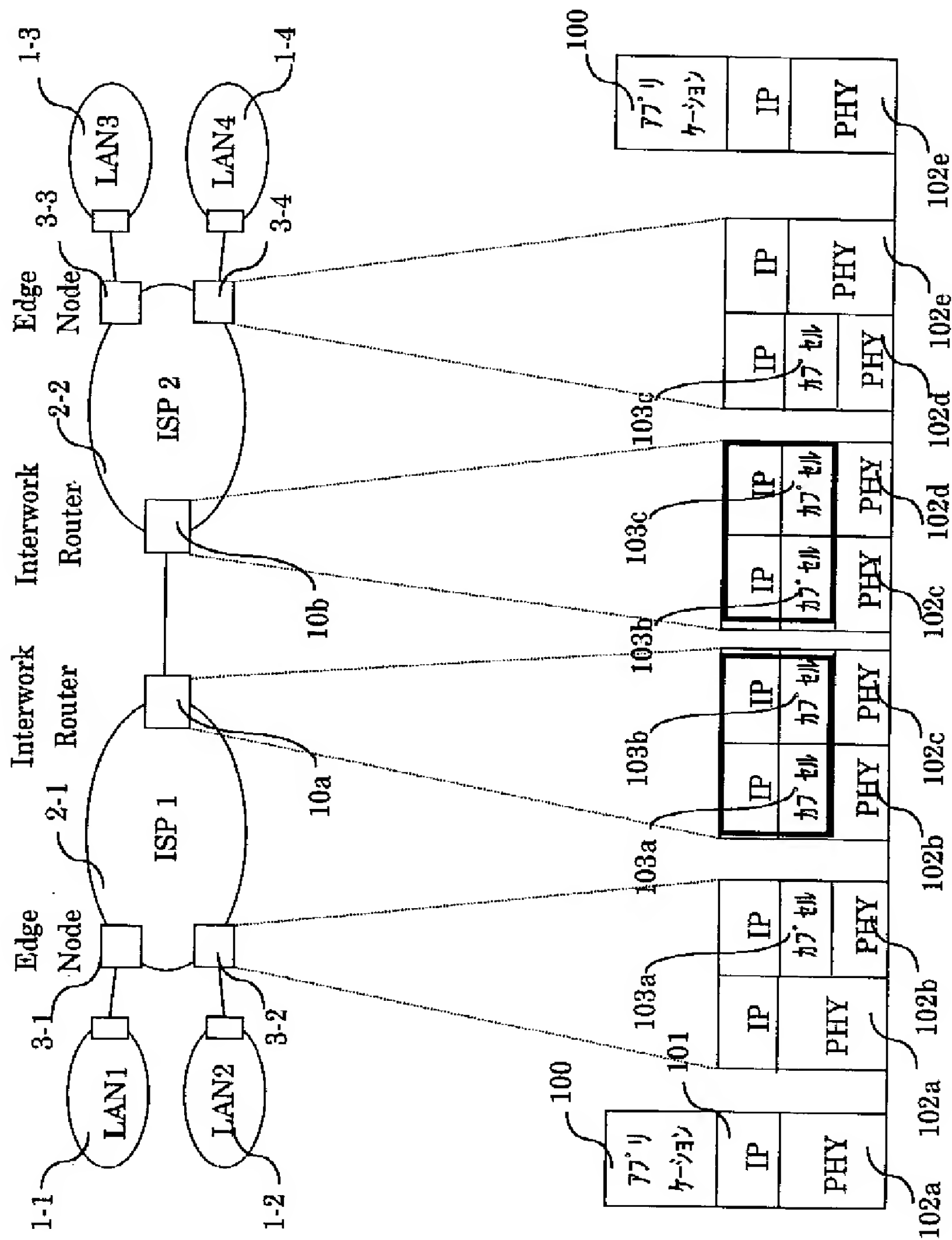
| 出力側カプセル番号 | | 出力側IPカプセルヘッダ | 出力側MACアドレス |
|-----------|-----|--------------|------------|
| 下位レイヤ番号 | QoS | IPカプセルヘッダ | |
| 5 | 0 | a | あ |
| 7 | 0 | b | う |
| 13 | 0 | m | た |
| | 0 | n | い |

340 343 345

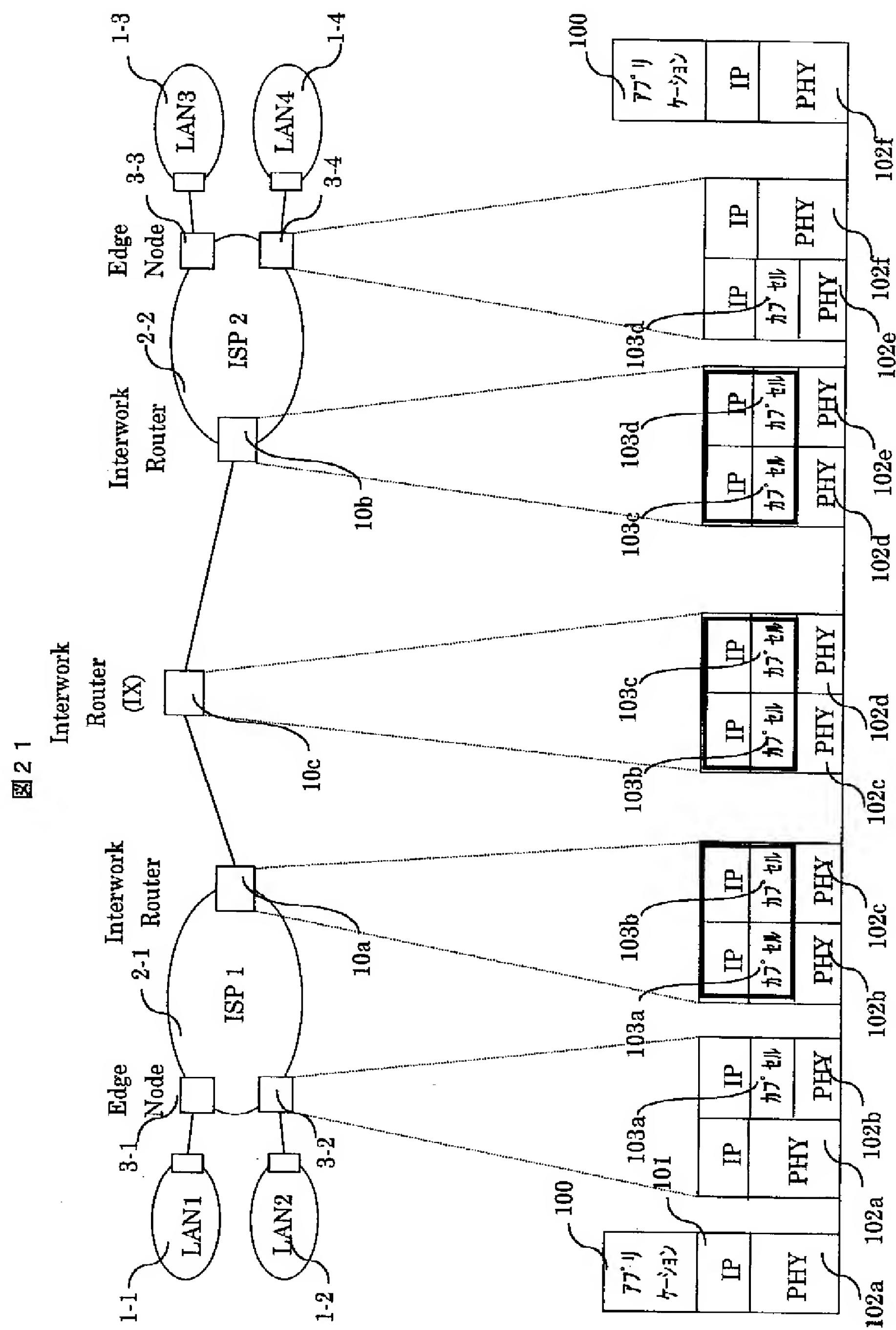
341 342 344

入力キー 出力キー

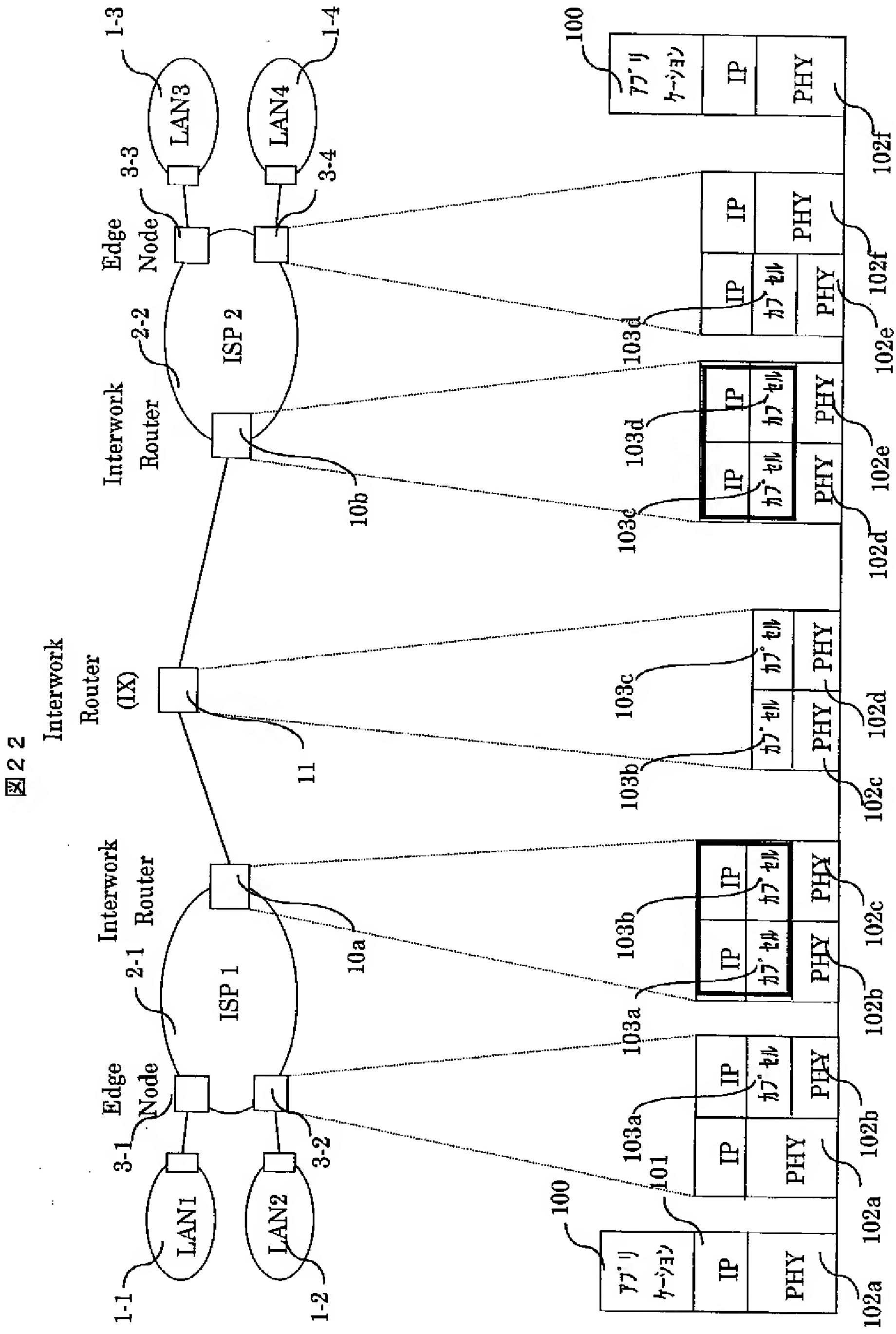
図 20



【図 2 1】

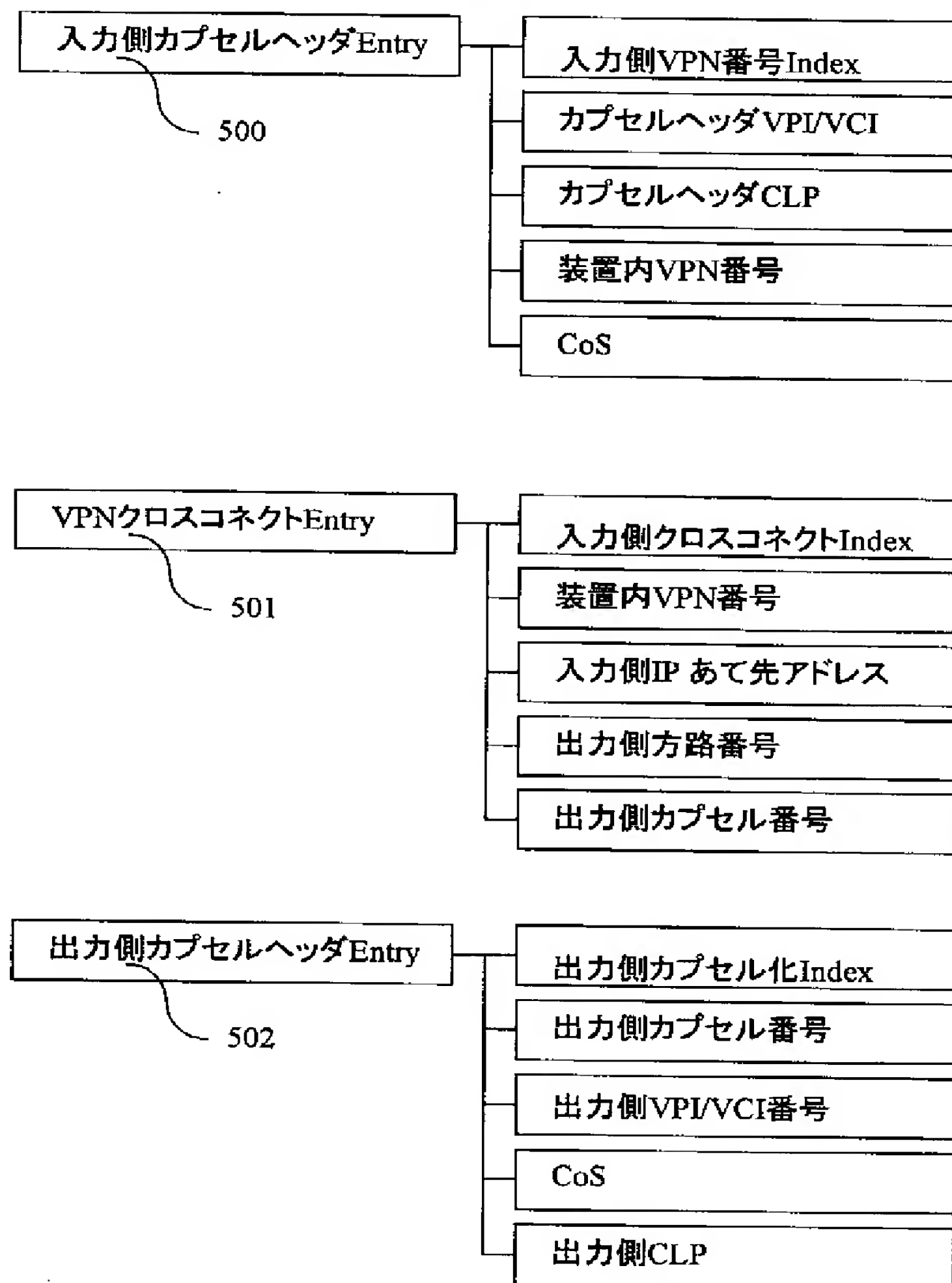


【図 2 2】



【図 2 3】

図23



【書類名】 要約書

【要約】

【課題】 複数インターネットサービスプロバイダ (ISP) にまたがる仮想専用網 (VPN: Virtual Private Network) を提供することである。

【解決手段】 両インターネットサービスプロバイダのネットワーク接続部分のインターワークゲートウェイにおいて、各パケットの方路を決定する際に、VPNを構成するために導入されるカプセル化ヘッダの領域とIPヘッダ両方の領域の情報をを用いて方路を決定し、更に出力側網におけるカプセル化ヘッダも前記情報から構成する。

【効果】 仮想専用線の相互接続が可能となり、複数インターネットサービスプロバイダにまたがるVPNを構成できる。また第一の網と第二の網のQoS情報をインターワークすることができる。

【選択図】 図1

【書類名】 手続補正書
【あて先】 特許庁長官殿
【事件の表示】
【出願番号】 平成11年特許願第147663号
【補正をする者】
【識別番号】 000005108
【氏名又は名称】 株式会社日立製作所
【代理人】
【識別番号】 100075096
【弁理士】
【氏名又は名称】 作田 康夫
【手続補正1】
【補正対象書類名】 明細書
【補正対象項目名】 発明の名称
【補正方法】 変更
【補正の内容】
【発明の名称】 データ転送装置

【手続補正2】
【補正対象書類名】 明細書
【補正対象項目名】 特許請求の範囲
【補正方法】 変更
【補正の内容】

【特許請求の範囲】

【請求項1】

第一のカプセル化ヘッダを用いて構成された第一の仮想閉域網と第二のカプセル化ヘッダを用いて構成された第二の仮想閉域網とに接続されたデータ転送装置であって、上記第一の仮想閉域網から第一のカプセル化ヘッダによってカプセル化されたデータを受信し、上記第二の仮想閉域網に第二のカプセル化ヘッダによってカプセル化された上記データを送信する送受信部と、上記第一のカプセル化ヘッダと上記データ内のヘッダの情報とから生成した上記第二のカプセル化ヘッダを上記データに付与し、さらに上記第一のカプセル化ヘッダと上記データ内のヘッダの情報とから決定したデータ送出経路へ、上記第二のカプセル化ヘッダを付与した上記データを出力するパケット処理部を備えたデータ転送装置。

【請求項2】

請求項1記載のデータ転送装置であって、上記送受信部は、上記第二の仮想閉域網から上記第二のカプセル化ヘッダによってカプセル化されたデータを受信し、上記第一の仮想閉域網に上記第一のカプセル化ヘッダによってカプセル化された上記データを送信し、上記パケット処理部は、上記第二のカプセル化ヘッダと上記データ内のヘッダの情報とから生成した上記第一のカプセル化ヘッダを上記データに付与し、さらに上記第二のカプセル化ヘッダと上記データ内のヘッダの情報とから決定したデータ送出経路へ、上記第一のカプセル化ヘッダを付与した上記データを出力することを特徴とするデータ転送装置。

【請求項3】

請求項1記載のデータ転送装置であって、上記データはインターネットプロトコルに準拠したデータであることを特徴とするデータ転送装置。

【請求項4】

請求項1記載のデータ転送装置であって、上記第一及び第二のカプセル化ヘッダは、インターネットプロトコルに準拠したカプセル

化ヘッダであることを特徴とするデータ転送装置。

【請求項 5】

請求項 1 記載のデータ転送装置であって、

上記第一及び第二のカプセル化ヘッダは、A T M通信方式に準拠したヘッダであることを特徴とするデータ転送装置。

【請求項 6】

請求項 1 記載のデータ転送装置であって、

上記第一及び第二のカプセル化ヘッダは、H D L C通信方式に準拠したヘッダであることを特徴とするデータ転送装置。

【請求項 7】

請求項 1 記載のデータ転送装置であって、

上記第一及び第二のカプセル化ヘッダは、M P L S通信方式に準拠したヘッダであることを特徴とするデータ転送装置。

【請求項 8】

請求項 1 記載のデータ転送装置であって、

上記第一のカプセル化ヘッダ内には、上記第一の仮想閉域網で使用する上記データの第一の転送優先度の情報が含まれており、

上記第二のカプセル化ヘッダ内には、上記第二の仮想閉域網で使用する上記データの第二の転送優先度の情報が含まれており、

上記パケット処理部は、上記第一のカプセル化ヘッダ内の上記第一の転送優先度の情報を上記第二の転送優先度の情報に変換して上記第二のカプセル化ヘッダ内に格納することを特徴とするデータ転送装置。

【請求項 9】

請求項 1 記載のデータ転送装置であって、

上記データ処理部が、上記第一のカプセル化ヘッダと上記データ内のヘッダの情報とからインデックスを生成し、該インデックスに基づいて上記第二のカプセル化ヘッダを生成し、また該インデックスに基づいて上記データ送出経路を決定することを特徴とするデータ転送装置。

【請求項 1 0】

請求項 1 記載のデータ転送装置であって、

上記データ処理部は、第一の下位レイヤ処理部と、該第一の下位レイヤ処理部に接続された第一のパケットレイヤ処理部と、該第一のパケットレイヤ処理部に接続されたスイッチと、該スイッチに接続された第二のパケットレイヤ処理部と、該第二のパケットレイヤ処理部に接続された第二の下位レイヤ処理部を有し、

上記データを受信した上記第一の下位レイヤ処理部では、上記第一のカプセル化ヘッダから装置内入力V P N番号を生成し、上記装置内入力V P N番号と上記データとを上記第一のパケットレイヤ処理部へ転送し、

上記第一のパケットレイヤ処理部では上記装置内入力V P N番号と上記データ内のヘッダの情報とから出力方路番号及び装置内出力V P N番号を決定し、

上記スイッチでは、上記出力方路番号に基づいて上記第二のパケットレイヤ処理部を選択し、該第二のパケットレイヤ処理部を介して上記装置内出力V P N番号と上記データとを上記第二の下位レイヤ処理部へ転送し、

上記第二の下位レイヤ処理部では、上記装置内出力V P N番号に基づいて上記第二のカプセル化ヘッダを生成し、該第二のカプセル化ヘッダを上記データに付与して出力することを特徴とするデータ転送装置。

【請求項 1 1】

請求項 1 0 記載のデータ転送装置であって、

上記装置内入力V P N番号及び上記装置内出力V P N番号の情報内にはQ o Sフィールドが設けられており、

上記第一の下位レイヤ処理部は、上記第一のカプセル化ヘッダ内のQ o S情報に基づいて

上記装置内入力VPN番号の情報内のQoSフィールドに値を書き込み、
上記第一のパケットレイヤ処理部は、上記装置内入力VPN番号の情報内のQoSフ
ィールドの値に基づき、上記装置内出力VPN番号の情報内のQoSフ
ィールドに値を書き込
み、

上記第二の下位レイヤ処理部は、上記装置内出力VPN番号の情報内のQoSフ
ィールドの値に基づき、上記第二のカプセル化ヘッダ内にQoS情報を書き込むことを特徴とする
データ転送装置。

【請求項12】

請求項1記載のデータ転送装置であって、

上記第一のカプセル化ヘッダはATMヘッダであり、上記第二のカプセル化ヘッダはIP
カプセル化ヘッダであり、

上記データ処理部は、上記ATMヘッダ内のCLPビットの値に基づき、上記IPカプセ
ル化ヘッダ内のTOSフィールドに値を書き込むことを特徴とするデータ転送装置。

【請求項13】

請求項2記載のデータ転送装置であって、

上記第一のカプセル化ヘッダはATMヘッダであり、上記第二のカプセル化ヘッダはIP
カプセル化ヘッダであり、

上記データ処理部は、上記IPカプセル化ヘッダ内のTOSフィールドの値に基づき、上
記ATMヘッダ内のCLPビットの値を書き込むことを特徴とするデータ転送装置。

【書類名】 手続補正書
【あて先】 特許庁長官 殿
【事件の表示】
【出願番号】 平成11年特許願第147663号
【補正をする者】
【識別番号】 000005108
【氏名又は名称】 株式会社日立製作所
【代理人】
【識別番号】 100100310
【弁理士】
【氏名又は名称】 井上 学

【手続補正1】
【補正対象書類名】 明細書
【補正対象項目名】 特許請求の範囲
【補正方法】 変更
【補正の内容】

【特許請求の範囲】

【請求項1】

第一のカプセル化ヘッダを用いて構成された第一の仮想閉域網と第二のカプセル化ヘッダを用いて構成された第二の仮想閉域網とに接続されたデータ転送装置であって、

上記第一の仮想閉域網から第一のカプセル化ヘッダによってカプセル化されたデータを受信し、上記第二の仮想閉域網に第二のカプセル化ヘッダによってカプセル化された上記データを送信する送受信部と、

上記第一のカプセル化ヘッダと上記データ内のヘッダの情報とから生成した上記第二のカプセル化ヘッダを上記データに付与し、さらに上記第一のカプセル化ヘッダと上記データ内のヘッダの情報とから決定したデータ送出経路へ、上記第二のカプセル化ヘッダを付与した上記データを出力するパケット処理部を備えたデータ転送装置。

【請求項2】

請求項1記載のデータ転送装置であって、

上記送受信部は、上記第二の仮想閉域網から上記第二のカプセル化ヘッダによってカプセル化されたデータを受信し、上記第一の仮想閉域網に上記第一のカプセル化ヘッダによってカプセル化された上記データを送信し、

上記パケット処理部は、上記第二のカプセル化ヘッダと上記データ内のヘッダの情報とから生成した上記第一のカプセル化ヘッダを上記データに付与し、さらに上記第二のカプセル化ヘッダと上記データ内のヘッダの情報とから決定したデータ送出経路へ、上記第一のカプセル化ヘッダを付与した上記データを出力することを特徴とするデータ転送装置。

【請求項3】

請求項1記載のデータ転送装置であって、

上記データはインターネットプロトコルに準拠したデータであることを特徴とするデータ転送装置。

【請求項4】

請求項1記載のデータ転送装置であって、

上記第一及び第二のカプセル化ヘッダは、インターネットプロトコルに準拠したカプセル化ヘッダであることを特徴とするデータ転送装置。

【請求項5】

請求項1記載のデータ転送装置であって、

上記第一及び第二のカプセル化ヘッダは、ATM通信方式に準拠したヘッダであることを特徴とするデータ転送装置。

【請求項6】

請求項1記載のデータ転送装置であって、

上記第一及び第二のカプセル化ヘッダは、HDL C通信方式に準拠したヘッダであることを特徴とするデータ転送装置。

【請求項 7】

請求項 1 記載のデータ転送装置であって、

上記第一及び第二のカプセル化ヘッダは、MPL S通信方式に準拠したヘッダであることを特徴とするデータ転送装置。

【請求項 8】

請求項 1 記載のデータ転送装置であって、

上記第一のカプセル化ヘッダ内には、上記第一の仮想閉域網で使用する上記データの第一の転送優先度の情報が含まれており、

上記第二のカプセル化ヘッダ内には、上記第二の仮想閉域網で使用する上記データの第二の転送優先度の情報が含まれており、

上記パケット処理部は、上記第一のカプセル化ヘッダ内の上記第一の転送優先度の情報を上記第二の転送優先度の情報に変換して上記第二のカプセル化ヘッダ内に格納することを特徴とするデータ転送装置。

【請求項 9】

請求項 1 記載のデータ転送装置であって、

上記パケット処理部が、上記第一のカプセル化ヘッダと上記データ内のヘッダの情報とからインデックスを生成し、該インデックスに基づいて上記第二のカプセル化ヘッダを生成し、また該インデックスに基づいて上記データ送出経路を決定することを特徴とするデータ転送装置。

【請求項 10】

請求項 1 記載のデータ転送装置であって、

上記パケット処理部は、第一の下位レイヤ処理部と、該第一の下位レイヤ処理部に接続された第一のパケットレイヤ処理部と、該第一のパケットレイヤ処理部に接続されたスイッチと、該スイッチに接続された第二のパケットレイヤ処理部と、該第二のパケットレイヤ処理部に接続された第二の下位レイヤ処理部を有し、

上記データを受信した上記第一の下位レイヤ処理部では、上記第一のカプセル化ヘッダから装置内入力VPN番号を生成し、上記装置内入力VPN番号と上記データとを上記第一のパケットレイヤ処理部へ転送し、

上記第一のパケットレイヤ処理部では上記装置内入力VPN番号と上記データ内のヘッダの情報とから出力方路番号及び装置内出力VPN番号を決定し、

上記スイッチでは、上記出力方路番号に基づいて上記第二のパケットレイヤ処理部を選択し、該第二のパケットレイヤ処理部を介して上記装置内出力VPN番号と上記データとを上記第二の下位レイヤ処理部へ転送し、

上記第二の下位レイヤ処理部では、上記装置内出力VPN番号に基づいて上記第二のカプセル化ヘッダを生成し、該第二のカプセル化ヘッダを上記データに付与して出力することを特徴とするデータ転送装置。

【請求項 11】

請求項 10 記載のデータ転送装置であって、

上記装置内入力VPN番号及び上記装置内出力VPN番号の情報内にはQoSフィールドが設けられており、

上記第一の下位レイヤ処理部は、上記第一のカプセル化ヘッダ内のQoS情報に基づいて上記装置内入力VPN番号の情報内のQoSフィールドに値を書き込み、

上記第一のパケットレイヤ処理部は、上記装置内入力VPN番号の情報内のQoSフィールドの値に基づき、上記装置内出力VPN番号の情報内のQoSフィールドに値を書き込み、

上記第二の下位レイヤ処理部は、上記装置内出力VPN番号の情報内のQoSフィールドの値に基づき、上記第二のカプセル化ヘッダ内にQoS情報を書き込むことを特徴とするデータ転送装置。

【請求項 1 2】

請求項 1 記載のデータ転送装置であって、

上記第一のカプセル化ヘッダは A T Mヘッダであり、上記第二のカプセル化ヘッダは I Pカプセル化ヘッダであり、

上記パケット処理部は、上記 A T Mヘッダ内の C L Pビットの値に基づき、上記 I Pカプセル化ヘッダ内の T O Sフィールドに値を書き込むことを特徴とするデータ転送装置。

【請求項 1 3】

請求項 2 記載のデータ転送装置であって、

上記第一のカプセル化ヘッダは A T Mヘッダであり、上記第二のカプセル化ヘッダは I Pカプセル化ヘッダであり、

上記パケット処理部は、上記 I Pカプセル化ヘッダ内の T O Sフィールドの値に基づき、上記 A T Mヘッダ内の C L Pビットの値を書き込むことを特徴とするデータ転送装置。

出願人履歴

000005108

19900831

新規登録

508277874

東京都千代田区神田駿河台4丁目6番地

株式会社日立製作所

000005108

20040908

住所変更

508277874

東京都千代田区丸の内一丁目6番6号

株式会社日立製作所